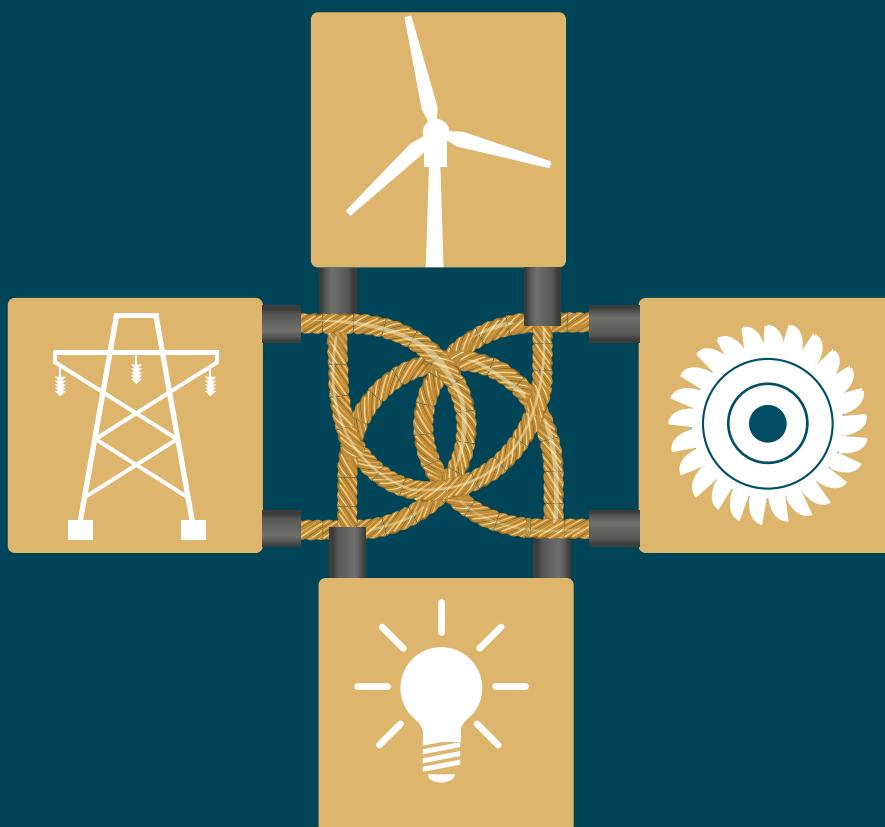




Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen

1
2013

V E I L E D E R



Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen

(beredskapsforskriften)

Veileder nr 1-2013

Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør: Ingvild Vaggen Malvik

Forfattere: Truls Sønsteby, Frank Skapalen, Helge Ulsberg, Roger Steen, Arthur Gjengstø, Anne Rogstad, Ann-Kristin Larsen, Rikke C. Arnulf, Sverre Sivertsen og Ingvild Vaggen Malvik.

Trykk: Kun på internett

Opplag: Utgave 1. juli 2013

Forsideill.: NVE

ISSN 1501-0678

Sammendrag: Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).

Emneord: Beredskap, sikkerhet, forebyggende sikkerhet, risiko- og sårbarhetsanalyse, varsling, rapportering, øvelse, ekstraordinære situasjoner, KBO, KSL, reparasjonsberedskap, ressurser, personell, transport, klassifisering, informasjonssikkerhet, taushetsplikt, sikkerhetsavtale, personkontroll, besøksrestriksjoner, driftskontroll, driftssentral, SCADA, AMS, samband, driftsradio, EMP, EMI.

Norges vassdrags- og energidirektorat
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 22 95 95 95
Telefaks: 22 95 90 00
Internett: www.nve.no

Juli 2013

Innhold

Kapittel 1. Innledende bestemmelser	9
§ 1-1. Formål	9
§ 1-2. Virkeområde	9
§ 1-3. Hvem forskriften er rettet mot	12
Kapittel 2. Generelle krav	13
§ 2-1. Ansvar	14
§ 2-2. Organisasjon og funksjon	14
§ 2-3. Beredskapsplikt	16
§ 2-4. Risiko- og sårbarhetsanalyse	17
§ 2-5. Beredskapsplanlegging	20
§ 2-6. Varsling og rapportering	22
§ 2-7. Øvelser	25
§ 2-8. Informasjonsberedskap	26
§ 2-9. Evaluering	27
§ 2-10. Internkontrollsystem	27
Kapittel 3. Kraftforsyningens beredskapsorganisasjon (KBO).....	29
§ 3-1. Organisering av KBO	29
§ 3-2. Beredskapsmyndigheten	30
§ 3-3. KBO-enheter	31
§ 3-4. Ansvar og oppgaver for KBO-enhetene	32
§ 3-5. Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig.....	33
§ 3-6. Ansvar og oppgaver for kraftforsyningens distriktssjefer	34
§ 3-7. Fritaksordninger	35
Kapittel 4. Ressurser og reparasjonsberedskap	37
§ 4-1. Reparasjonsberedskap	37
§ 4-2. Kompetanse og personell	38
§ 4-3. Drift i ekstraordinære situasjoner og gjenoppretting av funksjon ..	40
§ 4-4. Materiell og utstyr	48
§ 4-5. Transport	51
§ 4-6. Nasjonal tungtransportberedskap	53
§ 4-7. Samband	54
Kapittel 5. Klassifisering og sikringstiltak	57
§ 5-1. Sikringsplikt	57
§ 5-2. Klasser	63
§ 5-3. Sikring av klassifiserte anlegg	71
§§ 5-4, 5-5 og 5-6. Sikringstiltak for klasse klasse 1-3	72
Del I Fysisk utførelse - beskyttelse	76
Del II Uønskede hendelser og handlinger skal oppdages	99
Del III Effektiv gjenoppretting og reparasjonsberedskap	102
Del IV Redundans i anlegg og system	104

Del V Anleggenes egen strømforsyning, nødstrøm	107
Del VI Kompetent bemanning av anlegg	115
Del VII Krav til alternativ drift og beredskapsrom	116
Del VIII Øvrige tiltak	120
Del IX Kraftledninger	121
Del X Fjernvarmesentral mv.	125
§ 5-7. Vedtak om sikring eller klasse	125
§ 5-8. Analyse	126
§ 5-9. Meldeplikt om sikringstiltak	127
§ 5-10. Vakt hold	128
§ 5-11. Besøksrestriksjoner	129
Kapittel 6. Informasjonssikkerhet	133
§ 6-1. Identifisering av sensitiv informasjon og rettmessige brukere	134
§ 6-2. Sensitiv informasjon	137
§ 6-3. Beskyttelse, avskjerming og tilgangskontroll	142
§ 6-4. Sikkerhetsinstruks	143
§ 6-5. Anskaffelser i energiforsyningen	144
§ 6-6. Begrenset anbudsinnbydelse	145
§ 6-7. Personkontroll	145
§ 6-8. Sikkerhetskopier	147
Kapittel 7. Beskyttelse av driftskontrollsystem	149
§ 7-1. Generell plikt til å beskytte driftskontrollsystemet	149
§ 7-2. Overordnede sikkerhetsregler	157
§ 7-3. Dokumentasjon av driftskontrollsystemet	158
§ 7-4. Kontroll med brukertilgang	159
§ 7-5. Kontroll ved endringer i driftskontrollsystemet	160
§ 7-6. Kontroll med utstyr i driftskontrollsystemet	161
§ 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd	164
§ 7-8. Beredskap og alternativ drift ved svikt i driftskontrollsystemet ...	165
§ 7-9. Bemanning av driftssentral	166
§ 7-10. Ekstern tilkobling til driftskontrollsystem	167
§ 7-11. Systemredundans i driftskontrollsystemet	170
§ 7-12. Sammenkobling mellom avanserte måle- og styringssystem (AMS) og driftskontrollsystem	171
§ 7-13. Beskyttelse mot elektromagnetisk puls og interferens	172
§ 7-14. Særskilte krav til driftskontrollsystem i klasse 2	173
§ 7-15. Særskilte krav til driftskontrollsystem klasse 3	189
§ 7-16. Vern av kraftsystem i regional- og sentralnettet	195
§ 7-17. Mobile radionett – driftsradio	196
Kapittel 8. Avsluttende bestemmelser	199
§ 8-1. Kontroll	199
§ 8-2. Pålegg	200
§ 8-3. Dispensasjon	201
§ 8-4. Tvangsmulkt	201
§ 8-5. Overtredelsesgebyr	202
§ 8-6. Straff	203

§ 8-7. Gebyr til beredskapsmyndigheten.....	203
§ 8-8. Ikraftreden	203
§ 8-9. Forholdet til eldre vedtak om klassifisering og overgangsregler ..	204
9. Litteratur	207
10. Forskriftstekst	211
VEDLEGG 1 – 14.	244

Forord

Samfunnet er avhengig av stabile leveranser av elektrisitet og fjernvarme. Kraftforsyning er en av samfunnets aller viktigste infrastrukturer, og dette forplikter. Gjennom forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften, bfe) stilles det klare krav til alle enheter innen kraftforsyningens beredskapsorganisasjon (KBO) om å arbeide systematisk med tiltak for å forebygge og håndtere ekstraordinære hendelser som kan skade eller hindre produksjon, overføring eller fordeling av elektrisk energi eller fjernvarme.

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen trådte i kraft 01.01.2013. Denne versjonen av veiledningen bygger på tidligere veiledning (NVE Veileder 1-2011), forarbeidene som ble publisert i NVE-rapport 62-2012, og på innspill NVE har fått fra bransjen gjennom seminarer som ble avholdt i februar og mars 2013. Beredskapsforskriften (bfe) av 2012 erstattet beredskapsforskriften (BfK) fra 2002. Den nye forskriften er tilpasset endringen av energiloven som ble vedtatt i 2012, jf prop. 112 L (2010-2011), Innst. 140 L (2011-2012), Lovvedtak 34 (2011-2012). Lovendringen innebar blant annet en ny bestemmelse i energiloven som slår fast at enhver plikter å hindre at andre enn rettmessige brukere får adgang og kjennskap til sensitiv informasjon om kraftforsyningen. Nærmere krav til informasjonssikkerhet er utdypet i bfe.

Bfe legger opp til en ny måte å klassifisere anlegg på. Etter den tidligere forskriften (BfK) ble alle anlegg klassifisert etter enkeltvedtak. I bfe er kriteriene for klassifisering forskriftsfestet, og vil være kjent for tiltakshavere i forkant av en konsesjonsprosess. NVE har fremdeles anledning til å fatte enkeltvedtak om opp- eller nedklassifisering av anlegg dersom dette er hensiktsmessig. For å oppfylle krav til sikring etter kapittel 5 en hensiktsmessig måte har NVE på utvalgte områder hvor det finnes relevante bransjenormer, henvist til disse. Veiledningen konkretiserer disse kravene (jf vedleggene til bfe). Videre understreker forskriften at dersom et minst like godt sikringsnivå kan dokumenteres, kan NVE akseptere andre sikringstiltak enn de som er beskrevet. Normalt kreves det heller ikke utført sikringstiltak som innebærer vesentlige ombygginger av eksisterende anlegg, med mindre anleggene er særlig viktige eller særlig dårlig sikret.

Beskyttelse av driftskontrollsystemer er viet et eget kapittel i bfe. Økt avhengighet av IKT tilsier økt oppmerksomhet rundt sikring av systemene som styrer energiforsyningen. Bfe legger også opp til en større grad av systematikk i beredskapsarbeidet gjennom krav til årlig gjennomgang av ROS-analyser og evalueringer etter ekstraordinære situasjoner og øvelser slik at beredskapskompetansen utvikles, og at risiko- og sårbarhetsanalyser og beredskapsplaner oppdateres og forbedres.

Sikkerhet og beredskap er et lederansvar. NVE forventer at KBO-enhetenes øverste ledelse sørger for å formidle og følge opp beredskapsforskriftens bestemmelser på alle måter. I dette arbeidet håper vi at denne veiledningen vil være et nyttig verktøy.

Oslo, juli 2013



Per Sanderud

vassdrags- og
energidirektør

Om beredskapsforskriften og veiledningen

Hjemmel:

Fastsatt av Norges- vassdrags- og energidirektorat 7. desember 2012 med hjemmel i lov 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) §§ 9-1, 9-2 og 9-3 og forskrift 7. desember 1990 nr. 959 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskriften) § 9-1, gitt med hjemmel i energiloven § 10-6.

Hensikten med forskrift om forebyggende sikkerhet og beredskap i kraftforsyningen (beredskapsforskriften, bfe) er å stille krav som kan sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en sikker og effektiv måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene.

Dette innebærer at det stilles en rekke minimumskrav til alle enheter i kraftforsyningens beredskapsorganisasjon (KBO) om forebygging og håndtering av ekstraordinære hendelser som kan skade eller hindre produksjon, overføring eller fordeling av elektrisk kraft og fjernvarme.

Forskriften fra 2012 er en kombinasjon av funksjonelle og overordnede krav og mer detaljerte krav. Veiledningen utdypet og forklarer forskriftsteksten.

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen med veiledning gjelder også for fjernvarmeanlegg. Enkelte krav til fysisk sikring (jf kapittel 5) lar seg imidlertid ikke oppfylle uten videre for denne typen anlegg. NVE vil komme tilbake til en nærmere omtale av krav til sikring av fjernvarmeanlegg i en senere publikasjon.

Utforming av veiledningen

Der det står **må** eller **skal** i veiledningen, viser det direkte til krav stilt i beredskapsforskriften. Dette er absolutte krav. Der det i veiledningen står **må minst** eller **må som minimum**, angir dette et minimumsnivå for å oppfylle forskriftens krav. Enheten må da etterleve disse kravene.

Der det står **kan** eller **bør** i veiledningen, er dette anbefalinger/forslag og eksempler på hvordan krav til funksjon og overordnede mål kan løses for å oppfylle forskriftens krav.

Forebyggende og beredskapsmessige tiltak skal bygge på fastsatte krav, samt egne målsettinger og risikovurderinger ut over dette. Risikovurderingene og valg av tiltak ut over minimumskravene, må hele tiden tilpasses endringer i trusselbildet, teknologi og organisasjon.

Hvis enheten velger en annen løsning enn den som er beskrevet i veiledningen, eller hvis gjennomført risiko- og sårbarhetsanalyser tilsier at det er behov for en løsning med høyere ytelsesnivå, må det kunne dokumenteres at valgt løsning er like bra eller bedre enn

den som er beskrevet i veiledningen. ROS-analyser kan med andre ord ikke gi grunnlag for å anvende løsninger som innebærer et lavere ytelsesnivå enn beskrevet i veilederen.

Forskriftsteksten står gjennomgående i kursiv. Den etterfølgende teksten er veiledning som gir utfyllende kommentarer til hvordan forskriftens bestemmelser kan oppfylles. Grå tekstbokser gir eksempler. Navn på lover og andre relevante forskrifter som det henvises til, står også i kursiv. For oversikt og nærmere referanser henvises det til litteraturliste i kapittel 9.

Når det henvises til andre paragrafer i beredskapsforskriften, vil kun paragrafen bli skrevet, for eksempel: jf § 2-6 Varsling og rapportering. Dersom det henvises til andre lover og forskrifter, vil dette stå foran paragrafen, for eksempel: se *energiloven* § 6-1 Systemansvaret.

Veiledningen må leses som et helhetlig dokument. Eksempelvis ligger ikke alle kravene til driftskontrollsystemer i kapittel 7, krav til sikringsnivå vil følge av kapittel 5. Kravet til ROS-analyser omfatter mange bestemmelser i forskriften, blant annet skal man gjennomføre ROS-analyse for samband og transportberedskap. Veiledningen er samtidig strukturert slik at den er egnet som oppslagsverk, med krysshenvisninger til relevante bestemmelser.

Ingen av listene i denne veiledningen er uttømmende, og det vil alltid være ekstra lokale forhold som må vurderes og legges til. Slike forhold skal avdekkes i ROS-analysene.

Ved manglende oppfyllelse av krav, kan NVE fatte vedtak i medhold av *energiloven* og forskrifter.

Kapittel 1. Innledende bestemmelser

§ 1-1. Formål

Innenfor formålene i energiloven § 1-2, skal forskriften sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene.

1.1.1 Hensikten med bestemmelsen

Beredskapsforskriftens formål ligger innenfor energilovens formålsbestemmelse. Formålsbestemmelsen angir at beredskap er en del av det å realisere energilovens formål. Formålet med energiloven er å "sikre at produksjon, omforming, overføring, omsetning, fordeling og bruk av energi foregår på en samfunnsmessig rasjonell måte, herunder skal det tas hensyn til allmenne og private interesser som blir berørt", jf enl § 1-2.

Det er også ønskelig å angi formålet med beredskapsforskriften særskilt. Beredskapsforskriften har som mål at energiforsyningen også opprettholdes i ekstraordinære situasjoner, inkludert evnen til å gjenopprette energiforsyningen, slik at kundene får energi.

1.1.2 Nærmere om ekstraordinære hendelser og situasjoner

Formålsparagrafen angir at det er samfunnsmessige hensyn som ligger til grunn for kravet om at energiforsyningen både skal være i stand til å forebygge og håndtere ekstraordinære situasjoner. Se for øvrig også veiledning til § 4-1. Hva som er ekstraordinært, er ofte situasjonsbetinget, men i grove trekk kan man forklare begrepet med en uønsket hendelse som går utover de feilsituasjoner som selskapet håndterer til daglig. Under arbeidet med å identifisere uønskede hendelser er det viktig å skille mellom årsak (eks: storm/uvær) og uønsket hendelse (eks: havarert mast). En ekstraordinær hendelse kan forårsake en ekstraordinær situasjon, som et større avbrudd i energiforsyningen.

Et annet eksempel er utbrudd av pandemisk influensa, hvor mange av de ansatte i energiforsyningen blir syke på samme tid. En pandemi vil kunne forårsake en ekstraordinær situasjon, selv om ikke dette i seg selv forårsaker brudd på forsyningen. Men ekstraordinært stort sykefravær kan true evnen til gjenoppretting dersom dette medfører mangel på kvalifisert personell.

Kravet til å opprettholde energiforsyningen gjelder også i ekstraordinære situasjoner.

§ 1-2. Virkeområde

Forskriften gjelder forebygging, håndtering og begrensnings av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring og fordeling av elektrisk energi eller fjernvarme.

1.2.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å presisere virkeområdet til forskriften, og slik avgrense den fra energilovens generelle virkeområde, som er mer omfattende.

1.2.2 Nærmere om forebygging, håndtering og begrensning av virkninger

NVE legger til grunn at ordet «virkninger» i denne sammenhengen er i tråd med formuleringen i energiloven.

Med uttrykket ”ekstraordinære situasjoner” angir forskriften at det ikke er rettet mot drift i normalsituasjoner. Kravene i beredskapsforskriften pålegger imidlertid plikter som må oppfylles mens det er normal driftsituasjon og før det er oppstått en ekstraordinær situasjon. Dette gjelder eksempelvis forebyggende sikkerhet i driftskontrollsystemer. Under ordinær drift kan det dessuten oppstå driftsforstyrrelser og feil. Dette skal håndteres i henhold til kravene som stilles etter blant annet *leveringskvalitetsforskriften* og *systemansvarsforskriften* for normalsituasjoner.

Virkeområdet omfatter *alle former* for ekstraordinære situasjoner som kan *skade* eller *hindre* energiforsyningen, slik som for eksempel naturgitte skader, omfattende teknisk svikt og påført skade. Disse eksemplene vil vi utdype i den etterfølgende teksten.

1.2.3 Nærmere om naturgitt skade

Naturgitt skade omfatter alle former for konsekvenser av hendelser som skriver seg fra uvær, flom, skred og liknende. Det vil kunne være en gråson mellom det ordinære og ekstraordinære som for eksempel en vanlig norsk vinter vs. ekstremvær. For en nærmere vurdering av naturgitte forhold som NVE anser som ekstraordinære, anbefaler vi å lese veiledningen i sammenheng.

Når det gjelder naturgitte forhold, kan man for flere områder komme fram til relativt pålitelige anslag for risiko basert på erfaringer og statistikk. Nye forhold som for eksempel effekten av framtidige klimaendringer må samtidig tas med i vurderingen. Det kan skape større grad av usikkerhet, noe som også må vektlegges.

Eksempler på naturgitte forhold:

- Uvær – for eksempel sterk vind utover det som er normalt i området.
- Ising av linjer
- Skred
- Flom
- Skogbrann
- Lyn
- Trefall og vegetasjonstilvekst

1.2.4 Nærmere om omfattende teknisk svikt

Omfattende teknisk svikt omfatter hendelser som kan skyldes at tekniske komponenter ikke holder tilfredsstillende standard, eller at de ikke tåler påkjenninger som de blir utsatt for. Her vil det i mange tilfeller kunne være en sammenheng mellom naturgitt skade og teknisk svikt, siden komponenter kan havarere som følge av dårlig vær. I tilfeller hvor komponenter blir utsatt for påkjenninger som de skal kunne tåle, vil det være et tilfelle av teknisk svikt.

Eksempler på teknisk svikt:

- Bortfall av strøm og kjøling.
- Feil i maskiner og utstyr - fysiske feil.
- Feil i data eller programvare - logiske feil.
- Feil pga systemtekniske svakheter.
- Brann og eksplosjon.
- Lekkasje/oversvømmelse.
- Feil knyttet til svekkelse av komponenter på grunn av alder eller temperaturer, eller menneskelige svikt i forhold til rutiner/operasjoner.

1.2.5 Nærmere om omfattende påført skade

Påført skade omfatter alle typer kriminelle handlinger (hærverk, sabotasje mv), i tillegg til skade som påføres anlegget på grunn av menneskelig feil (graveskader, feilkoblinger mv). Påført skade omfatter derfor både skade som er påført med hensikt om å skade anlegget, og skade som blir påført som følge av uaktsomhet og kompetansesvikt.

Tilsiktede handlinger

Konsekvensene av tilsiktede handlinger kan bli store for virksomheten og samfunnet. Her må man se nærmere på hvor stor sannsynlighet det er for å utføre tilsiktede handlinger. Stor grad av sannsynlighet og store konsekvenser vil fortelle mye om sårbarhetsbildet for det enkelte objektet. Tilsiktede handlinger kan være mer eller mindre rasjonelle handlinger - og omfatte alt fra nøye planlagt sabotasje - til tilfeldig skadeverk.

Eksempler på tilsiktede handlinger:

- Kriminelle handlinger og skadeverk.
- Ulike former for industrispionasje.
- Sabotasje/terror.
- Skade fra krigsliknende handlinger.

1.2.6 Nærmere om informasjonssikkerhet

Forskriften gjelder også for informasjonssikkerhet. Det vil si sikkerhet for at ikke andre enn rettmessige brukere får tilgang til sensitiv informasjonen om energiforsyningen. Det er i *energilovent* § 9-3 tredje ledd gitt en særskilt forskriftshjemmel for informasjonssikkerhet og taushetsplikt. Energilovens bestemmelse om taushetsplikt favner videre enn de øvrige bestemmelsene om beredskap fordi den gjelder for ”enhver”. Informasjonssikkerhet beholdes som del av beredskapsforskriften.

Kapittel 6 i forskriften og veiledning til kapittel 6 utdyper hvordan dette skal forstås.

1.2.7 Forskriften omfatter fjernvarme

Virkeområdet bygger dessuten på at beredskapsforskriften gjelder for beredskap i forbindelse med alle former for elektrisk energiproduksjon, inkludert gasskraft og vindkraft og fjernvarme. Dette er i samsvar med *energilovent* kapittel 9. For å tydeliggjøre dette, brukes uttrykket ”energiforsyningen” i denne bestemmelsen og i andre bestemmelser i beredskapsforskriften. Dette gjelder selv om energilovent kapittel 9

enkelte steder har beholdt uttrykket ”kraftforsyningen”, men forutsetter at dette uttrykket tolkes slik at det inkluderer fjernvarme.

§ 1-3. Hvem forskriften er rettet mot

Forskriften gjelder for de virksomheter som etter § 3-3 er enheter i Kraftforsyningens beredskapsorganisasjon (KBO). Forskriften gjelder også for de virksomheter som etter vedtak blir KBO-enheter.

Forskriftens kapittel 5 gjelder for de virksomheter som eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme.

Forskriftens § 6-2 om taushetsplikt for sensitiv informasjon gjelder for enhver.

1.3.1 Hensikten med bestemmelsen

Bestemmelsen klargjør hvilke juridiske enheter som er innenfor forskriftens virkeområde, det vil si hvem den gjelder for.

1.3.2 Nærmere om hvem som er omfattet av forskriften

Forskriften retter seg i første rekke mot de virksomheter som er KBO-enheter som nærmere beskrevet i kapittel 3. Kraftforsyningens beredskapsorganisasjon (KBO) benyttes fortsatt både i energiloven og i beredskapsforskriften, selv om den også omfatter fjernvarme (jf veiledning til § 1-2).

En nærmere veiledning om hvem som er KBO-enheter er omtalt under § 3-3 KBO-enheter.

Kravene i kapittel 5 gjelder for de virksomheter som eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme, også for virksomheter som ikke er KBO-enheter. Dette innebærer for eksempel at krav til sikring også gjelder for anlegg som kan bli av vesentlig betydning, selv om de per 2012 ikke er klassifisert. For øvrig vises det til kapittel 5, og særlig §§ 5-1, 5-8 og 5-9.

Bestemmelsen i § 6-1 om taushetsplikt for sensitiv informasjon gjelder for enhver, det vil si alle som måtte få tilgang til sensitiv informasjon om energiforsyningen. Dette har selvstendig hjemmel i *energiloven* § 9-3. Reglene om informasjonssikkerhet er taushetspliktregler, og innebærer at enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om energiforsyningen. Rettmessige brukere vil primært være selskapets egne ansatte, innleide leverandører og myndigheter med tilsynsansvar på området. Dette er nærmere beskrevet i veiledningen til kapittel 6 i forskriften.

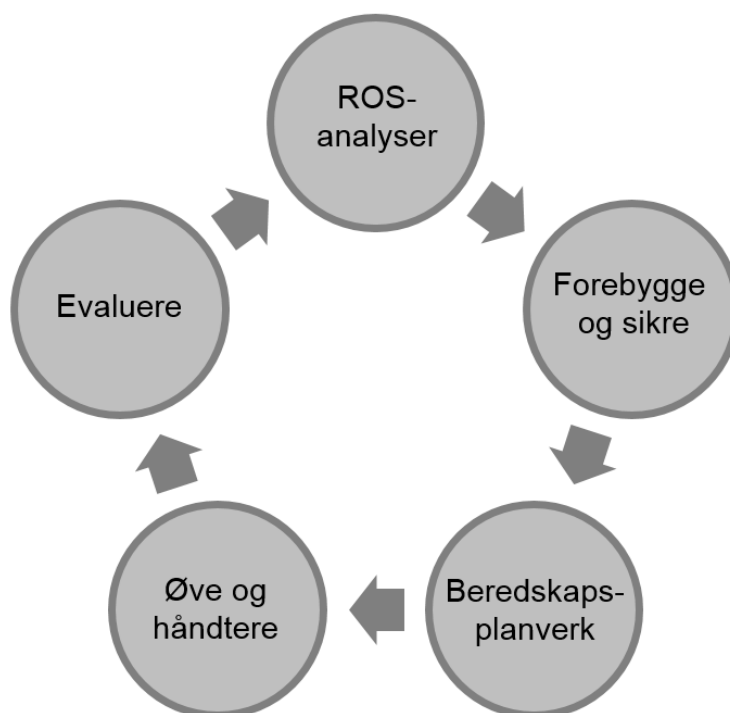
Kapittel 2. Generelle krav

Kapittel 2 beskriver grunnleggende krav til virksomhetene som er omfattet av forskriften, for å sikre at beredskapsarbeidet er helhetlig og funksjonelt, kontinuerlig og forankret i ledelsen.

Som det går fram av formålet §1-1, skal forskriften sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner. Hensikten er å redusere de samfunnsmessige konsekvensene av manglende energiforsyning. En forutsetning for at selskapene skal være i stand til å håndtere ekstraordinære situasjoner, er at de har et helhetlig beredskapskonsept.

KBO-enhetene skal bruke ROS-analyser som planverktøy for å skaffe seg grunnlag for å utarbeide gode beredskapsplaner og kunne prioritere ressursene til de viktigste tiltakene. Disse analysene skal sette virksomhetene i stand til å vurdere hvilke hendelser som kan forebygges, og hvilke sikringstiltak som kan iverksettes for å forhindre, eller begrense skadevirkningene av ekstraordinære hendelser. Hendelser som ikke kan forebygges, eller hvor det gjenstår en restrisiko, skal omtales i beredskapsplanverket. Slike hendelser skal håndteres i henhold til beredskapsplanverket, og håndteringen skal øves jevnlig av virksomheten. Håndtering av ekstraordinære hendelser og øvelser skal evalueres, og sammen med nye trusselvurderinger, tilsyn fra beredskapsmyndigheten med videre skal virksomheten vurdere om det er nødvendig med en oppdatering av ROS-analysene.

Figur 2-1 Et helhetlig beredskapskonsept.



§ 2-1. Ansvar

Leder for virksomhet som er omfattet av denne forskrift har ansvar for at:

a. Virksomheten har en organisasjon med de funksjoner som kreves i denne forskrift, og at det er etablert klare ansvars- og myndighetsforhold.

b. Virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift.

c. Kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift oppfylles.

d. Internkontroll etableres og praktiseres.

2.1.1 Formålet med bestemmelsen

Bestemmelsen beskriver hva leder for virksomheten har ansvar for. Leder for virksomheten vil i de fleste tilfeller være daglig leder (eller tilsvarende) av KBO-enheten, men det kan også være den daglige leder (eller tilsvarende) av virksomheter som ikke er en KBO-enhet (jf sikringsplikten, se § 5-1).

2.1.2 Ansvar og myndighet

Leder for virksomhetens ansvar for å oppfylle energiloven og beredskapsforskriften er tydeliggjort gjennom bestemmelsen. Bestemmelsen forankrer ansvar for et helhetlig beredskapsarbeid hos daglig leder for virksomheten på en entydig måte. Dette er imidlertid ikke til hinder for at eier er ansvarlig.

Leder for virksomheten kan ikke delegere ansvaret som følger av bestemmelsen. Hvordan den ansvarlige lederen delegerer myndighet og oppgaver i egen organisasjon er det opp til lederen å avgjøre, så lenge bestemmelsene blir fulgt opp.

§ 2-2. Organisasjon og funksjon

Virksomhet som omfattes av denne forskrift skal ha følgende funksjoner:

a. Beredskapsleder. Denne utpekes av leder for virksomheten og skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet.

b. Beredskapskoordinator. Denne skal være administrativt kontaktpunkt til beredskapsmyndigheten.

c. IKT-sikkerhetskoordinator. Denne skal være faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet.

2.2.1 Formålet med bestemmelsen

Kravene etter denne bestemmelsen er fastsatt for å sikre at det blir utpekt personer i virksomhetene som skal ha et spesielt ansvar for at kravene i beredskapsforskriften etterleves. Videre er det viktig at NVE til enhver tid har en oppdatert oversikt over disse

nøkkelfunksjonene hos KBO-enhetene slik at kontakt raskt kan etableres i forbindelse med en ekstraordinær situasjon. For skjema for registrering av endringer av kontaktinformasjon, se vedlegg 10.

Videre er formålet med å utpeke beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator at KBO-enheten utvikler nødvendig kompetanse til å håndtere ulykker, skader og andre ekstraordinære situasjoner som truer energiforsyningen.

2.2.2 Nærmere om utpeking

Det framgår av bestemmelsen at virksomhetens leder er beredskapsansvarlig og har ansvaret for at det blir utpekt personer til å fylle funksjonene som følger av denne bestemmelsen. Leder skal selv utpeke beredskapsleder dersom dette er en annen person enn virksomhetens leder.

KBO-enhetene må ta hensyn til at kritisk viktige medarbeidere kan være forhindret fra å stille opp i en ekstraordinær situasjon og at en pågående hendelse kan vare over tid. NVE anbefaler derfor at KBO-enhetene også utpeker stedfortredere som kan fylle disse funksjonene.

2.2.3 Nærmere om leder for virksomheten

Leder for virksomheten har ansvar for at enheten etterlever beredskapsforskriftens krav. NVE forventer at vedkommende:

- Kjenner til kravene i beredskapsforskriften.
- Sørger for at enheten har kompetanse i hvordan kravene skal forstås og håndteres.
- Utpeker beredskapsleder (dersom det er en annen person enn leder selv), og sørge for at det blir utpekt beredskapskoordinator og IKT-sikkerhetskoordinator.
- Sørger for at det blir utpekt nødvendige stedfortredere.
- Er ansvarlig for at NVE blir holdt løpende oppdatert om hvem som til enhver tid fyller de ulike funksjoner.
- Er ansvarlig for at henvendelser og vedtak fattet av NVE blir fulgt opp av virksomheten.

2.2.4 Nærmere om beredskapsleder

Beredskapsleder skal planlegge og utøve beredskapsarbeidet. NVE forventer at vedkommende:

- Har inngående kunnskap om gjeldende lover og forskrifter innenfor forebyggende sikkerhet og beredskap i energiforsyningen, inkludert kravene i beredskapsforskriften.
- Har kjennskap til energiforsyningen.
- Har god oversikt over enhetens beredskapsstatus og beredskapsorganisasjon.
- Holder seg oppdatert innenfor forebygging, beredskap og krisehåndtering.
- Bidrar til at henvendelser og vedtak fattet av NVE blir fulgt opp av virksomheten.

2.2.5 Nærmere om beredskapskoordinator

Alle enheter i KBO skal ha en beredskapskoordinator. Beredskapskoordinatoren er enhetens administrative kontaktledd mot beredskapsmyndigheten.

Beredskapskoordinators rolle utover å være myndighetskontakt avgjøres av virksomheten. NVE forventer at vedkommende:

- Har inngående kunnskap om gjeldende lover og forskrifter innenfor forebyggende sikkerhet og beredskap i energiforsyningen, inkludert kravene i beredskapsforskriftens. Beredskapskoordinator trenger likevel ikke ha detaljkunnskaper innenfor hvert enkelt område.
- Har god oversikt over interne krav til KBO-enhetenes sikkerhets- og beredskapsarbeid.
- Koordinerer formidling av informasjon, henvendelser og vedtak fra beredskapsmyndigheten internt i virksomheten.
- Bidrar til at henvendelser fra beredskapsmyndigheten blir fulgt opp av virksomheten.

2.2.6 Nærmere om IKT-sikkerhetskoordinator

Alle enheter i KBO skal ha en IKT-sikkerhetsskoordinator. IKT-sikkerhetsskoordinator er enhetens administrative kontaktledd mot beredskapsmyndigheten for IKT-relaterte utfordringer.

IKT-sikkerhet blir stadig viktigere for virksomhetene, og det er viktig for etterlevelse av bestemmelsene i denne forskriften at virksomhetene har en fagressurs med god kompetanse om både IKT-sikkerhet og IKT-beredskap. Det er et ledelsesansvar å sørge for at IKT-sikkerhetskoordinator har eller får tilført denne kompetansen.

IKT-sikkerhetskoordinators rolle utover å være myndighetskontakt avgjøres av virksomheten. NVE forventer at vedkommende:

- Har inngående kunnskap til gjeldende lover og forskrifter innenfor IKT-sikkerhet og beredskap i energiforsyningen, inkludert kravene i beredskapsforskriften..
- Har god oversikt over interne krav til KBO-enhetenes IKT-sikkerhets- og beredskapsarbeid.
- Koordinerer formidling av informasjon, henvendelser og vedtak fra beredskapsmyndigheten med betydning for IKT-sikkerhet internt i virksomheten.
- Bidra til at henvendelser fra beredskapsmyndigheten om IKT-sikkerhet tema blir fulgt opp av virksomheten.
- Kan koordinere planlegging, gjennomføring og oppfølging av virksomhetens arbeid med beskyttelse av driftskontrollsystem og virksomhetens øvrige IKT-system som inneholder sensitiv informasjon om energiforsyningen.
- Har god kunnskap om enhetens driftskontrollfunksjoner og administrative datasystemer, deres funksjonalitet, og hvordan de skal beskyttes.
- Har god kjennskap til IKT-trusselbildet.

§ 2-3. Beredskapsplikt

Virksomhet som er omfattet av denne forskrift, skal sørge for effektiv sikring og beredskap, og skal iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner i samsvar med energiloven § 9-2 første ledd.

2.3.1 Hensikten med bestemmelsen

Bestemmelsen presiserer den generelle plikten til å arbeide med forebyggende sikkerhet og beredskap. *Energiloven* § 9-2 første ledd sier følgende:

”Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner som nevnt i § 9-1 fjerde eller femte ledd og for å gjenopprette normal situasjon” (vår understrekning).

Dette betyr at alle virksomheter som er regulert av denne bestemmelsen skal *sørge for effektiv sikring og beredskap*, blant annet gjennom tilstrekkelig forebyggende tiltak og reparasjonsberedskap mv.

2.3.2 Nærmere om beredskapsplikt

Beredskapsplikten gjelder for ekstraordinære situasjoner. For nærmere klargjøring av hva som regnes som ekstraordinære situasjoner, se veiledning til § 1-1. Beredskap for ekstraordinære situasjoner omfatter både tiltak for å forebygge, håndtere og begrense virkningene. Mange av disse tiltakene må nødvendigvis både planlegges og gjennomføres i en normalsituasjon. Et eksempel på dette er tiltak knyttet til IKT-sikkerhet og informasjonssikkerhet. Men også fysisk sikring av anlegg vil være et viktig virkemiddel for å forebygge og begrense virkningene av ekstraordinære situasjoner.

Plikten hviler på alle som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning. Dette innebærer at dette kravet gjelder flere enn dem som er KBO-enheter, jf også § 5-1. Plikten følger også av § 3-5 bokstav c og § 5-3 bokstav c Beredskap, som er likelydende bestemmelser og som angir plikter for konsesjonærer for henholdsvis elektriske anlegg og fjernvarme: *”Konsesjonæren plikter ved planlegging, utførelse og drift av anlegget å sørge for at det tas beredskapsmessige hensyn”*.

Beredskapsforskriften og denne veiledningen beskriver hvordan plikten til å ta beredskapsmessige hensyn i praksis skal og kan oppfylles.

§ 2-4. Risiko- og sårbarhetsanalyse

Alle KBO-enheter skal gjennomføre risiko- og sårbarhetsanalyser knyttet til ekstraordinære forhold. Analysene skal ha et slikt omfang at enheten kan identifisere risiko og sårbarhet ved alle funksjoner, anlegg og tiltak av betydning for å oppfylle kravene i forskriften. Analysene skal minimum gjennomgås årlig og oppdateres ved behov.

2.4.1 Hensikten med bestemmelsen

Gode risiko- og sårbarhetsanalyser vil hjelpe KBO-enhetene med å identifisert risiko- og sårbarhet som kan redusere eller true virksomhetens evne til å fungere. Formålet med å identifisere risiko og sårbarhet ved ekstraordinære hendelser knyttet til teknisk svikt, naturgitt skade eller påført skadeverk er å sortere mellom det som kan forebygges, for eksempel gjennom sikringstiltak, og det som må håndteres ved hjelp av beredskapsplanverket.

Videre skal virksomheten også kunne ha oversikt over egen sårbarhet, for eksempel når flere hendelser opptrer på samme tid. Gode risiko- og sårbarhetsanalyser vil bidra til å redusere antall og omfang av ekstraordinære hendelser, samt redusere konsekvensene av

slike hendelser. ROS-analysene kan ikke brukes til å redusere beredskapen under forskriftens minimumskrav til sikring.

Se også § 5-8 Analyse for krav til virksomheter som planlegger å bygge eller vesentlig endre eller utvide klassifiserte anlegg.

2.4.2 Nærmere om innhold i analysene

Bestemmelsen klargjør at alle KBO-enheter skal gjennomføre risiko- og sårbarhetsanalyser knyttet til ekstraordinære forhold. Dette betyr at fokus legges mye på forhold som kan gi stor konsekvens for virksomheten og/eller samfunnet, men ikke nødvendigvis være i den kategorien som oppfattes å ha en høy sannsynlighet for å inntreffe.

Det framgår av bestemmelsen at ”Analysene skal ha et slikt omfang at enheten kan identifisere risiko og sårbarhet ved alle funksjoner, anlegg og tiltak av betydning for å oppfylle kravene i forskriften.” Analysen skal av den grunn favne oversikt over risiko på overordnet nivå, i forhold til alle relevante objekter, systemer og funksjoner av betydning for forsyningssikkerheten. Og ikke minst også dekke alle beredskapsplikter gitt i denne forskriften.

Eksempler på ekstraordinære forhold (jf § 5-1):

- Uvær og annen naturgitt skade
- Brann og eksplosjoner
- (Alvorlig) teknisk svikt (IKT, driftskontrollsystem)
- Innbrudd, hærværk, sabotasje og andre kriminelle handlinger

Det er viktig å ta høyde for flere samtidige hendelser, og hendelser kan vare i lang tid. Tilgang på personell, ressurser og infrastruktur kan være begrenset, for eksempel som følge av pandemi eller utfall av ekom.

Det følger av bestemmelsen at det ikke bare dreier seg om én analyse, men en rekke analyser. Omfanget av analysearbeidet vil variere fra virksomhet til virksomhet. Den enkelte analysen skal belyse risiko- og sårbarhet både for hele virksomheten og for de vesentligste objektene, systemene, funksjonene og beredskapsordningene.

Bestemmelsen forutsetter at virksomhetene har god oversikt over egne anlegg og hvilke ekstraordinære hendelser som kan inntreffe. Kompleksiteten i energisystemet som den enkelte virksomhet har ansvaret for, vil være avgjørende for omfanget av analysene. NVE forventer god kvalitet på de analysene som KBO-enheterne utarbeider. Analysene vil legge føringer for (nye) sikringsbehov, beredskapsplan, øvelser og faktisk krisehåndtering. Behovet for **kompetanse** i egne rekker både for å forstå forskriften og velge ROS-metode er viktig. Virksomhetsledelsens egen **kompetanse til å kunne bestille slike tjenester** må også være tilstede dersom virksomheten velger å kjøpe tjenestene. For mer om kompetanse, se veiledning til § 4-2.

Alle ROS-analyser skal dateres når de er ferdigstilt og godkjent i virksomheten (jf § 2-10 Internkontroll). Det skal også framgå hvem som har godkjent analysen og hva en

eventuell gjennomgang/vurdering/oppdatering faktisk har medført og når den ble foretatt. Tidligere utgaver av analysene skal være sporbare i virksomhetens arkiv.

Analysene skal oppdateres ved behov. Det betyr ikke nødvendigvis at virksomhetene årlig skal utarbeide helt nye ROS-analyser for alle objekter, system osv. Men virksomhetene pålegges å gjøre minimum én årlig kvalitativ vurdering av analysenes relevans og tilstrekkelighet. Hvis det har skjedd vesentlige endringer, for eksempel knyttet til ytre omgivelser, internt i virksomheten, tilknytning av kunder (samfunnsmessige endringer), underleveranser eller hendelser som tilsier et oppdateringsbehov, skal det gjennomføres nye risiko- og sårbarhetsanalyser som fanger opp dette.

Analysene skal oppdateres på bakgrunn av:

- Erfaringer fra hendelser
- Erfaringer fra øvelser
- Endringer i nett, produksjon eller forbrukspunkter
- Nye trusselvurderinger
- Pålegg etter tilsyn

I tillegg skal analysene alltid oppdateres både før og etter strukturelle, teknologiske eller organisatoriske endringer. Uansett skal KBO-enheten gjennomgå ROS-analysene årlig. Det betyr at den enkelte analyses dato ikke skal overskride 365 dager.

2.4.3 Nærmere om metode for ROS-analyser

Risiko- og sårbarhetsanalyser er på mange måter det viktigste elementet i virksomhetens risikostyring. Overordnet analyse danner grunnlag for mer detaljerte analyser.

ROS- analyser kan identifisere svake sider ved energiforsyningsanlegg, energiforsyningsens ledelse, infrastruktur, teknologi, materiell, personell osv., som skal følges opp med forebyggende og beredskapsmessige tiltak. Hva KBO-enheten skal analysere, vil avhenge av både teknisk utforming av energianleggene, geografisk beliggenhet og organisatoriske forhold.

Forskriften stiller ikke eksplisitt krav til å bruke en bestemt metode. Men analysene skal tematisk dekke både risiko og sårbarhet. NVE har utarbeidet en metodeveiledning og eksempelsamling som kan hjelpe KBO-enhetene med dette arbeidet (NVE-Veileder 2-2010).

2.4.3.1 Analyse

Risiko- og sårbarhetsanalysene skal være systematiske og omfatte hele virksomheten og ta for seg de hendelsene som kan hindre en sikker energiforsyning under ekstraordinære forhold.

2.4.3.2 Forankring og samarbeid

Analysen må forankres hos virksomhetens ledelse. Det er viktig at relevant fagkompetanse i virksomheten blir involvert i arbeidet med analysene, spesielt personer

med inngående kjennskap til de anleggene som analyseres. Ekstern kompetanse kan også benyttes, men det er viktig at analysene tar utgangspunkt i de(t) spesifikke anlegg(ene), og ikke bare er en generell beskrivelse av mulige risiko- og sårbarhetsforhold. NVE anbefaler at KBO-enhetene har god kontakt med eksterne samarbeidspartnere, slik som offentlige myndigheter, politi, brannvesen, og samfunnskritiske funksjoner/virksomheter for øvrig.

Bestemmelsen om beredskapsplanlegging (§ 2-5) stiller krav om at beredskapsplanverket skal samordnes med berørte myndigheter og andre relevante virksomheter. NVE vil derfor anbefale at dialogen med øvrige aktører starter allerede i forbindelse med ROS-analysen(e).

2.4.3.3 Beslutning og oppfølging

Resultatet av analysene må følges opp, enten gjennom sikringstiltak (som helt eller delvis forebygger hendelsen), eller gjennom et beredskapsplanverk som forteller hvordan en hendelse, hvis den skjer, skal håndteres. Gode ROS-analyser kan også være verdifulle bidrag til den generelle planleggingen i selskapet med hensyn til organisering, ansvarsfordeling og nødvendige investeringer for å redusere risikoen til et akseptabelt nivå.

Oppfølging av ROS-analysene (som eksempelvis en handlingsplan) skal forelegges selskapets ledelse for beslutning. Handlingsplaner skal være konkrete og tidfestede, med prioritering av oppfølgingstiltak og ansvarlige for oppfølging.

§ 2-5. Beredskapsplanlegging

Alle KBO-enheter skal ha et oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang. Planverket skal bygge på risiko- og sårbarhetsanalyser og skal omfatte alle beredskapstiltak etter denne forskriften.

Beredskapsplanleggingen skal blant annet omfatte forberedelser og tiltak det kan bli nødvendig å iverksette ved store ulykker, vesentlige skader, trusselsituasjoner, rasjonering og andre ekstraordinære situasjoner som kan påvirke energiforsynings drift og sikkerhet. Beredskapsplanverket skal, innenfor rammene av kapittel 6 om informasjonssikkerhet, samordnes med berørte myndigheter og andre relevante virksomheter, deriblant andre KBO-enheter.

2.5.1 Hensikten med bestemmelsen

Bestemmelsen slår fast at den risiko- og sårbarhet som ikke virksomhetene kan fjerne eller redusere gjennom forebygging eller sikringstiltak, må omtales og håndteres gjennom beredskapsplanverket. I bestemmelsen nevnes det flere eksempler på hendelser, som store ulykker, vesentlig skade, trusselsituasjoner og rasjonering, som aldri helt kan utelukkes. Listen av mulige hendelser er på ingen måte uttømmende. Bestemmelsen skal sikre at slike situasjoner håndteres på en god og effektiv måte, slik at konsekvensene for energiforsyningen blir minst mulig.

2.5.2 Nærmere om beredskapsplanlegging

Beredskapsplanlegging er en kontinuerlig prosess, og dette må KBO-enheten legge til rette for. Planverket er en dokumentasjon på at prosessen er på plass. Med oppdatert beredskapsplanverk menes at det selv med små endringer (for eksempel at en person på

en varslingsliste har sluttet), er behov for å oppdatere planene. Beredskapsplanverket skal alltid være oppdatert og være datert med siste revisjonsdato.

Beredskapsplanleggingen og –planverket skal være beredskapsansvarliges virkemiddel til å komme raskt i gang med krisehåndteringen.

Skal en beredskapsplan virke etter hensikten, må den være godt kjent og lett tilgjengelig for alle som skal bruke den. Planen bør derfor ikke sikkerhetsgraderes, med unntak av de delene som inneholder sikkerhetsgradert informasjon i henhold til *sikkerhetsloven* eller sensitiv informasjon i henhold til denne forskriften. Hele eller deler av planverket kan imidlertid være underlagt taushetsplikt etter denne forskriften og skal da håndteres i tråd med disse kravene.

KBO-enheten skal knytte beredskapsplanleggingen til en egen kartlegging (beredskapsanalyse) av alle beredskapskrav og –behov. Det vil si at beredskapsplanleggingen og -planverket i sum skal dekke alle beredskapsplikter etter forskriften. Funn i ROS-analysene som ikke helt kan forebygges, skal gjenspeiles i beredskapsplanverket, sammen med eventuell restrisiko etter at sikringstiltak er gjennomført.

Beredskapsplanverket skal, innenfor rammene av kapittel 6 om informasjonssikkerhet, samordnes med berørte myndigheter og andre relevante virksomheter, deriblant andre KBO-enheter og KDS. Relevante myndigheter vil blant annet være kommuner, fylkeskommune, fylkesmann, forsvar, politi, brann mv. Hva som er samfunnskritisk virksomhet, vil variere. Den enkelte KBO-enhet må sikre et godt samspill med relevante myndigheter i beredskapsplanleggingen for å identifisere virksomheter med samfunnsviktige funksjoner. Et generelt kjennetegn vil være virksomheter som har særlig stor og umiddelbar betydning for befolkningens trygghet (liv og helse). Andre relevante virksomheter vil være blant annet infrastrukturaktører. Det er spesielt varslingslister for hvordan man raskt kan komme i kontakt med KBO-enheten det kan være relevant å dele med for eksempel kommunen. Det er også viktig å ha en god dialog med eiere av spesielt viktige objekter (jf *sikkerhetsloven*).

Et beredskapsplanverk bør som et minimum inneholde:

- Hasteark/prosedyre som beskriver hvordan beredskapsorganisasjonen skal aktiviseres.
- Oversikt over egen organisasjon og ledelse (som beskrive ansvar og myndighet).
- Varslingsliste (med oversikt over interne og alle relevante eksterne).
- Prosedyre for samhandling med brann/redning, politi osv.
- Oversikt over ressurser (personell, materiell mv.) med kontaktinformasjon.
- Relevante delplaner/innsatsplaner for forskjellige hendelser og områder, for eksempel:
 - Reparasjonsberedskap.
 - Transportberedskap.

- o Plan for personellforsterkning.
 - o Informasjonsplan.
 - o Plan for terrydding.
 - o Andre forhold kan være plan for håndtering av teknisk svikt, IKT, sabotasje, forsterket vakthold mv.
- Diverse vedlegg (kart, oversikter, mv.).
 - Prosedyre for å varsle NVE om ekstraordinære forhold (jf §2-6).

§ 2-6. Varsling og rapportering

Alle KBO-enheter skal uten ugrunnet opphold varsle beredskapsmyndigheten om ekstraordinære situasjoner. Varslet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson.

Alle KBO-enheter skal uten ugrunnet opphold og senest innen tre uker skriftlig innrapportere følgende uønskede hendelser til beredskapsmyndigheten:

- a. Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS).*
- b. Innbrudd, hærværk, sabotasje eller andre kriminelle handlinger, eller forsøk på dette.*
- c. Mistenkelig adferd ved viktige anlegg av betydning for energiforsyningen.*
- d. Situasjoner hvor sensitiv informasjon om kraftforsyningen er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette.*
- e. Avbrudd i distribusjon av elektrisitet i mer enn to timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere.*
- f. Avbrudd i fjernvarmeforsyningen i mer enn 12 timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere.*
- g. Større havarier i sentral- og regionalnettet.*
- h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer.*

Beredskapsmyndigheten kan kreve rapportering av andre tilfeller av uønskede hendelser enn de som er nevnt i første og annet ledd.

Beredskapsmyndigheten kan også pålegge virksomheter som eier eller driver anlegg eller system, som er eller kan bli av vesentlig betydning for produksjon, omforming, omsetning eller fordeling av elektrisk energi og fjernvarme, å rapportere uønskede hendelser i samsvar med andre ledd.

2.6.1 Hensikten med bestemmelsen

Denne bestemmelsen gir KBO-enhetene to ulike plikter. Den første er å varsle når noe ekstraordinært skjer. Den andre er å rapportere etter at hendelsen er over.

Hensikten med bestemmelsen er å sikre at NVE får relevante varsel om ekstraordinære situasjoner som kan ha betydning for drift og sikkerhet i energiforsyningen. Varsling av pågående ekstraordinære situasjoner legger til rette for rask og effektiv håndtering av slike situasjoner i KBO-organisasjonen. Det er ikke en forutsetning for varslings- og rapporteringsplikten at situasjonen har medført avbrudd i forsyningen.

Hensikten med å rapportere i etterkant av en ekstraordinær situasjon er å gi NVE grunnlag for å se etter generelle mønstre utover det den enkelte KBO-enhet kan registrere. NVE rapporterer slike forhold tilbake til KBO, blant annet gjennom en årlig anonymisert hendelsesrapport. Rapporteringen blir også brukt til å vurdere justeringer i regelverk og tilsyn. I spesielle tilfeller kan ekstraordinære situasjoner videreformidles til politi eller andre relevante myndigheter, men da i samråd med det enkelte selskapet. Politiske myndigheter vil også kunne be om informasjon om ekstraordinære situasjoner.

2.6.2 Nærmere om varsling

KBO-enhetene skal varsle NVE om ekstraordinære situasjoner som gir eller kan gi store samfunnsmessige konsekvenser, konsekvenser for KBO-enheten og/eller for energisystemet. Bokstav a-h gir en indikasjon på hendelser som kan forårsake en ekstraordinær situasjon, men virksomheten må selv vurdere om det er andre situasjoner som beredskapsmyndigheten bør være kjent med. Videre må virksomheten selv vurdere om det dreier seg om en forventet eller en pågående situasjon (varsling), eller om det er en hendelse som er avdekket i etterkant (rapportering). Et eksempel på situasjoner hvor det kan være aktuelt å varsle er der man ser at nettet vil kunne påføres ekstraordinær belastning under N-0 drift. Et eksempel på en hendelse som avdekkes i etterkant, kan være forsøk på innbrudd i et anlegg.

Eksempler på situasjoner som skal varsles, er når store områder (mange kunder) er uten forsyning, når viktige samfunnsfunksjoner blir berørt når det er grunn til å anta at utfallet vil bli langvarig eller det er stor mediemessig oppmerksomhet rundt en situasjon. Normalt vil utfall som omfatter en hel kommune, være omfattet av varslingsplikten. Etter *lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivildforsvaret (sivilbeskyttelsesloven)* og *forskrift om kommunal beredskapsplikt* skal kommunene være forberedt på å håndtere uønskede hendelser og utarbeide lokale beredskapsplaner som blant annet skal inneholde evakueringsplaner og plan for befolkningsvarsling. NVE ønsker på denne bakgrunn varsel om større utfall som omfatter en kommunes kriseledelse.

Det skal varsles uten ugrunnet opphold. Det vil si så snart som praktisk mulig. Varslingsprosedyren skal inngå i KBO-enhetens beredskapsplanverk. Det er viktigere å håndtere en krise enn å varsle. Samtidig er det viktig for NVE å motta slike varsel fra KBO-enheter raskt, spesielt fordi det i en tidlig fase av større hendelser kan være utfordrende å skaffe oversikt over omfanget og forventet varighet.

Det stilles ikke strenge formkrav til et slikt varsel. Varsel kan formidles på telefon, e-post eller på annen måte KBO-enheten finner hensiktsmessig. NVE ser gjerne at rapporteringsskjema benyttes til varsling, se vedlegg 5. Mottatte varsel registreres hos NVE.

2.6.3 Nærmere om rapportering

Alle KBO-enheter skal uten ugrunnet opphold og senest innen tre uker skriftlig rapportere om de uønskede hendelsene. Det er laget egne skjema for formålet. Det framgår av bestemmelsens bokstav a-h hva som skal rapporteres. Beredskapsmyndigheten kan også på anmodning kreve rapportering av andre tilfeller av uønskede hendelser enn dem som er nevnt i bestemmelsens første og andre ledd. KBO-enheten kan også uoppfordret rapportere om forhold som de mener beredskapsmyndigheten bør gjøre oppmerksom på.

I noen tilfeller vil det være nødvendig for beredskapsmyndigheten å etterspørre ytterligere informasjon fra KBO-enhetene om hendelsen, ut over informasjonen som skal oppgis i henhold til rapporteringsskjemaet. I slike tilfeller vil NVE ta kontakt med KBO-enheten, og be om en nærmere skriftlig redegjørelse. Slike redegjørelser vil komme i tillegg til, og ikke i stedet for, det ordinære rapporteringsskjemaet. Rapporteringsskjema finnes i vedlegg 6 (teknisk svikt, uhell, ulykker, naturgitte forhold etc.) og vedlegg 7 (hendelser forårsaket av uvedkommende) til veiledningen.

2.6.4 Nærmere om krav til form og prosedyre

Skjema for varsling og rapportering er tilgjengelig på www.nve.no. Det er ikke noe krav om at varsling må skje ved hjelp av dette skjemaet, men skjemaet gir likevel en oversikt over hvilken informasjon som det vil være relevant å formidle til beredskapsmyndigheten.

Det forutsettes at den enkelte enhet i KBO etablerer klare prosedyrer i beredskapsplanverket for hvordan varsling og rapportering skal foregå og hvem som skal ivareta dette i den enkelte virksomhet. Dersom enheten er i tvil om en hendelse skal rapporteres eller ikke, oppfordres enheten til å ta direkte kontakt med NVE for å avklare dette.

KBO-enhetene skal rapportere til NVE i tillegg til, og ikke istedenfor, en eventuell anmeldelse til politiet.

Rapporten sendes per post til NVE Beredskapsseksjonen, eller per e-post til beredskapsrapportering@nve.no (passordbeskyttet/kryptert etter behov). Dersom det er viktig med rask kontakt, kan NVE nås på den døgnåpne beredskapstelefonen. I kontortid kan Beredskapsseksjonen kontaktes.

NVEs beredskapstelefon: 22 95 93 60 / 909 92 231

2.6.5 Rapporteringsplikt også for andre enn KBO

Beredskapsmyndigheten kan også pålegge andre virksomheter som eier eller driver anlegg eller system, som er eller kan bli av vesentlig betydning for produksjon, omforming, omsetning eller fordeling av elektrisk energi og fjernvarme, å rapportere uønskede hendelser i samsvar med bestemmelsen (jf andre ledd).

§ 2-7. Øvelser

Alle KBO-enheter skal gjennomføre øvelser med slikt innhold og omfang at enheten vedlikeholder og utvikler sin kompetanse til å håndtere alle aktuelle ekstraordinære situasjoner. Virksomheten skal ha en flerårig øvelsesplan og gjennomføre minimum én årlig øvelse.

2.7.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sikre at KBO-enheterne øver på å håndtere alle de aktuelle ekstraordinære situasjonene som risiko- og sårbarhetsanalysene har identifisert, forhold som omtales i beredskapsplanverket og viktige prosedyrer av betydning for å opprettholde forsyningssikkerheten. Øvelsene skal videre ha et slikt innhold og omfang at enheten vedlikeholder og utvikler sin kompetanse.

2.7.2 Nærmere om planlegging av øvelser

Virksomheten må ha oversikt over nå-tilstanden når det gjelder kompetanse i virksomheten (for nærmere beskrivelse om krav til kompetanse, se § 4-2). Med dette menes kompetanse i henhold til forsyningssikkerhet og beredskap og ivaretagelsen av bestemmelsen i denne forskriften, håndteringsevne i henhold til aktuelle scenarioer beskrevet i ROS-analysen og beredskapsplanverket med videre.

Omfanget av øvelser, mengde, lengde og innhold må tilpasses slik at øvelsene fungerer som et virkemiddel for å oppnå målet med å styrke kompetansen. KBO-enheten skal ha en flerårig øvelsesplan som henger sammen med målene for kompetanseutviklingen. *Planen bør dekke en fireårsperiode.*

Virksomheten må gjennom sin øvelsesplan ha tydelige mål for hva som ønskes oppnådd med øvelsesplanleggingen, øvelsene og evalueringene av disse.

Den enkelte øvingsplanen bør evalueres etter uløpet av virkeperioden.

Samøvelser med brannvesenet, Forsvaret og politiet med flere vil også være relevant. NVE har i samarbeid med DSB (jf Eltilsynet) fastsatt et eget øvingsdirektiv: *Direktiv for øvelser ved m.m. ved kraftforsyningsanlegg* (www.nve.no). Dette gir de ulike partene ved slike øvelser klare plikter og rettigheter og skal følges ved alle øvelser i forbindelse med høyspenningsanlegg (se også veiledning til § 5-10 Vakthold).

2.7.3 Nærmere om praktisk gjennomføring av øvelser

NVE anbefaler at det utarbeides en dreiebok til bruk i øvelser. Øvelsene skal dekke relevante tema i forhold til forskriftens virkeområde. Dette omfatter blant annet:

- Reparasjonsberedskap
- Informasjonsberedskap
- Mangel på personell (som følge av for eksempel skade/pandemi)
- IKT-hendelser
- Naturkatastrofer/ekstremvær
- Sabotasje

- Samtidige hendelser

Det er ingenting i veien for å **øve sammen med andre** så lenge målene med øvelsen, for virksomhetens del, oppfylles slik at øvelsen bidrar til at virksomheten utvikler sin kompetanse. Tvert imot kan samøvelser ofte være svært viktige og verdifulle.

Bestemmelsen gir en plikt til å gjennomføre minimum én årlig øvelse (innen forskriftens virkeområde og innenfor ett og samme kalenderår). Dersom behovet for å kunne opprettholde enhetens kompetanse til å håndtere alle aktuelle ekstraordinære situasjoner tilsier at det må gjennomføres hyppigere øvelser, bør dette framgå av øvingsplanen. Nødvendige øvelser skal tilrettelegges, planlegges, gjennomføres og evalueres.

Scenarioer

En risiko- og sårbarhetsanalyse vil være til stor hjelp for å avdekke hvilke scenarioer som er aktuelle i en øvelse, hvor ofte og under hvilke forhold. Også erfaringer fra tidligere øvelser, ulykker og "nestenulykker" vil kunne være med på å danne oversikt over aktuelle scenarioer. Når det gjelder beredskapsplanverket, informasjonsberedskapen, relevante sikringstiltak med videre, bør dette regelmessig testes under øvelsene.

§ 2-8. Informasjonsberedskap

Alle KBO-enheter skal ha en informasjonsplan og en effektiv informasjonsberedskap i ekstraordinære situasjoner. Dette skal blant annet omfatte informasjon internt i enheten, til berørte myndigheter, samfunnskritiske virksomheter, andre relevante KBO-enheter, publikum og media, samt råd til kunder. Informasjonsplanen skal inngå som del av beredskapsplanverket, øves jevnlig og evalueres.

2.8.1 Hensikten med bestemmelsen

Bestemmelsen skal sikre at alle KBO-enheter har en plan for hvordan de skal få formidlet informasjon til og kommunisere med de aktørene som har behov for dette i forbindelse med en ekstraordinær situasjon. Informasjon internt i enheten, til berørte myndigheter, samfunnskritiske virksomheter, andre relevante KBO-enheter, mediene og publikum/kunder skal bidra til at kriser håndteres på en mest mulig rasjonell måte av de som blir berørt.

2.8.2 Nærmere om informasjonsplanen

KBO-enhetens informasjonsplan skal være en del av beredskapsplanverket og være tilpasset slik at den kan brukes under de ulike ekstraordinære hendelsene KBO-enheten kan bli stilt overfor. Dette omfatter eksempelvis informasjonsbehovet som oppstår i tilfeller hvor deler av eller alle strømvhengige kommunikasjonsmidler ligger nede. Det er viktig å være bevisst på at denne bestemmelsen omfatter informasjon både internt og eksternt.

Informasjonsplanen skal kunne dekke informasjon:

- Internt i enheten.
- Til berørte myndigheter (kommuner osv.).
- Samfunnskritiske virksomheter (infrastrukturaktører vei, tele, helse osv.).

- Andre relevante KBO-enheter (inkludert KDS/NVE).
- Medier.
- Publikum /samt råd til kunder (med fokus på direkte berørte).

Informasjonsplanen skal øves jevnlig og evalueres. Informasjonsberedskapen skal også dekke situasjoner der det for eksempel er strømløst over et større område med utfordringer med tele og data/nettsider osv. KBO-enheten skal med andre ord ha en plan for hvordan informasjonen til publikum skal skje når alle tekniske kommunikasjonsmidler stopper opp. NVE vil anbefale at ulike deler av slike planer utvikles i samarbeid med relevante samarbeidspartnere.

Hva som vil være en samfunnskritisk virksomhet kan variere fra kommune til kommune. Men et generelt kjennetegn vil være virksomheter som har stor betydning for befolkningens trygghet (liv og helse).

§ 2-9. Evaluering

Alle KBO-enheter skal etter ekstraordinære situasjoner og øvelser gjennomføre en evaluering. Evalueringen skal brukes som grunnlag for at virksomhetens beredskapskompetanse utvikles, at risiko- og sårbarhetsanalyser og beredskapsplaner oppdateres, og at det gjennomføres konkrete beredskapstiltak for anlegg, drift, gjenoppretting og øvrige tiltak som oppfyller kravene i denne forskriften.

2.9.1 Hensikten med bestemmelsen

Evalueringer som virkemiddel skal være en sentral del i virksomhetens beredskapsarbeid. Alle erfarte hendelser og øvelser skal dokumenteres gjennom en evaluering.

Målet er å identifisere og tilbakeføre erfaringer fra hendelser og øvelser inn i planlegging av forebyggende sikkerhet og beredskapsplanverket. Evalueringer vil også være viktige i forhold til kommende ROS-analyser og øvelsesscenarioer.

Evalueringer er et virkemiddel for å oppnå både individuell og organisatorisk læring. Hensikten er å avdekke organisatoriske suksesser og feilgrep, og ikke minst, hvorfor det gikk slik.

Virksomheten må kunne dokumentere at resultatene fra evalueringen er videreført risiko- og sårbarhetsanalysene og beredskapsplanverket til virksomheten.

§ 2-10. Internkontrollsystem

Alle KBO-enheter skal ha et internkontrollsystem som dokumenterer at det er etablert en systematikk for å sikre etterlevelse av kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift.

Internkontrollsystemet skal gjenspeile faktisk tilstand, og skal inneholde dokumentasjon for at alle tiltak etter kravene i første ledd er på plass og fungerer etter sin hensikt.

Internkontrollsystemet skal være tilrettelagt for gjennomføring av tilsyn i samsvar med de krav som er stilt.

2.10.1 Hensikten med bestemmelsen

Denne bestemmelsen er tydelig på at KBO-enheten skal ha et etablert internkontrollsystem som gir en rask og korrekt oversikt over beredskapstilstanden i virksomheten og etterlevelse av kravene i beredskapsforskriften. Systemet skal være et oversikts- og styringsverktøy for virksomheten. Det samme systemet skal kunne gi tilsynsmyndigheten en rask og korrekt dokumentasjon over status i forhold til alle relevante bestemmelser etter denne forskriften. Bestemmelsen viderefører kravet om kvalitetssystem fra BfK (2002).

2.10.2 Nærmere om internkontrollsystemets omfang

Den enkelte virksomhet må selv bestemme hvor omfattende systemet skal være. Bestemmelsen gir ingen avgrensning med hensyn til å bruke eller tilpasse allerede etablerte internkontrollsystemer, så lenge bestemmelsens vilkår er oppfylt gjennom å dokumentere at alle krav til beredskap i lov og forskrift er oppfylt.

Internkontrollsystemet må for eksempel gi informasjon om når siste ROS-analyse ble utført for et anlegg eller system, hvem som godkjente analysen og hvem som deltok i arbeidet, hvor analysen ligger og hva som er neste planlagte revisjonsdato med videre.

Kapittel 3. Kraftforsyningens beredskapsorganisasjon (KBO)

Kraftforsyningens beredskapsorganisasjon (KBO) er beskrevet i energiloven § 9-1:

§ 9-1. (Kraftforsyningens beredskapsorganisasjon)

Kraftforsyningens beredskapsorganisasjon (KBO) består av de enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme. Beredskapsmyndigheten kan ved forskrift eller enkeltvedtak fastsette hvilke enheter som skal inngå i KBO.

Alle enheter i KBO skal sørge for at virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver etter dette kapitlet.

Beredskapsmyndigheten skal samordne beredskapsarbeid og utpeke den samlede ledelse i KBO.

I ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, kan KBO pålegges oppgaver og plikter. Det samme gjelder i ekstraordinære situasjoner hvor skade eller hindring som nevnt i første punktum har oppstått.

Beredskapsmyndigheten kan under beredskap og i krig underlegge kraftforsyningen KBO. Kraftforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves.

Ansvars-, rolle- og oppgavedelingen innenfor KBO bygger blant annet på at hver enkelt enhet i KBO har en selvstendig plikt til uoppfordret å fatte de nødvendige beslutningene og iverksette de tiltakene som kreves for å forebygge og håndtere ekstraordinære hendelser.

Forskriften gjelder også for fjernvarmeselskaper, og fjernvarmeselskap inngår også i KBO. Dette kapitlet viser bestemmelsene for hvordan kraftforsyningens beredskapsorganisasjon skal organiseres.

§ 3-1. Organisering av KBO

Kraftforsyningens beredskapsorganisasjon består av KBO-enhetene, kraftforsyningens distriktssjefer (KDS) og beredskapsmyndigheten, samt kraftforsyningens sentrale ledelse (KSL) når denne trer i kraft, jf. § 3-5.

3.1.1 Hensikten med bestemmelsen

Bestemmelsen beskriver hvem som er aktører i KBO.

3.1.2 Nærmere om KBO

KBO er en nasjonal organisasjon med en definert ledelse og struktur. Ledelsesstrukturen er nærmere beskrevet i dette kapitlet.

Medlemmer i KBO er større produsenter, nettselskaper, fjernvarmeselskaper og eventuelt andre virksomheter av vesentlig betydning for energiforsyningen. Se for øvrig veiledning til § 3-3.

KSL er nærmere beskrevet i § 3-5.

Statnett SF er enhet i KBO, og skal følge kravene som framgår av forskriften. Ved erklært beredskap, inngår Statnett i KSL fra det tidspunkt KSL blir etablert. Se for øvrig veiledning til § 3-5. Systemansvaret reguleres ikke av denne forskriften.

§ 3-2. Beredskapsmyndigheten

Beredskapsmyndigheten skal i samsvar med energiloven § 9-1 tredje ledd utpeke den samlede ledelse i KBO og samordne beredskapsarbeidet.

3.2.1 Hensikten med bestemmelsen

Bestemmelsen beskriver beredskapsmyndighetens (NVEs) rett og plikt til å utpeke ledelsen i KBO og samordne beredskapsarbeidet.

3.2.2 Nærmere om fullmakt fra OED

Olje- og energidepartementet (OED) har gjennom eget vedtak delegert rollen som beredskapsmyndighet for Norges energiforsyning til NVE, jf *Delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat*. NVE er beredskapsmyndighet etter kapittel 9 i *energiloven*, med unntak av § 9-1 siste ledd (jf § 3-5).

Beredskapsmyndighetens rolle i KBO innebærer ingen innskrenkning av beredskapsmyndighetens fullmakter etter kapittel 9 i *energiloven*.

3.2.3 Nærmere om samordning av beredskapsarbeidet

NVE skal utpeke den samlede ledelsen i KBO. Det gjelder spesielt Kraftforsyningens sentrale ledelse (KSL) og Kraftforsyningens distriktssjefer (KDS). Men hjemmelen gir ingen begrensning når det gjelder å utpeke ledelsesledd innenfor KBO. Videre kan NVE stille krav til KBO-enhetene, føre tilsyn, pålegge å gjøre analyser, gjennomføre øvelser med videre.

Alle KBO-enheter har ansvar for å sikre nødvendig samordning av beredskapsplanverket og tilrettelegge for rasjonelt samvirke i forbindelse med krisesituasjoner. Det gjelder særlig samordning og samvirke med tilgrensende KBO-enheter.

Alle KBO-enheter skal ha kommunikasjonsmidler som sikrer at de kan kommunisere løpende med NVE/KSL og KDS, jf § 4-7.

3.2.4 Nærmere om varslingsgang

NVE kan instruere underliggende i KBO om om varslingsgang og kommunikasjonsmidler. Dette er tiltak som kommer i tillegg til pliktene som den enkelte KBO-enhet har internt på eget ansvarsområde. NVE kan instruere underliggende ledd om å iverksette varslingsøvelser og gjennomføre varslinger. Den enkelte KBO-enhet plikter å svare på og rette seg pålegg uten ugrunnet opphold.

NVE kan også iverksette og gjennomføre særskilte beredskapstiltak ved ekstraordinære situasjoner. NVE kan ved behov kan delegere myndighet til underliggende ledd i KBO, blant annet KDS, jf § 3-6.

§ 3-3. KBO-enheter

KBO-enheter er de virksomheter som eier eller driver anlegg og som har konsesjon etter energiloven §§ 3-1, 3-2 eller 5-1, og som i medhold av § 5-2 eller § 5-7 er klassifisert etter denne forskrift.

Beredskapsmyndigheten kan ved enkeltvedtak bestemme at også andre virksomheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, skal være KBO-enheter.

3.3.1 Hensikten med bestemmelsen

Bestemmelsen definerer kriteriene for å være enhet i KBO. Virksomheter som oppfyller kriteriene i første ledd, blir automatisk medlem i KBO gjennom forskriften. I tillegg åpner andre ledd for at NVE kan vedta at også andre virksomheter skal være med i KBO, når dette er hensiktsmessig.

3.3.2 Nærmere om KBO-enhet etter forskrift

Første ledd i bestemmelsen innebærer at virksomheter automatisk inngår i KBO etter forskriften dersom de har minst ett klassifisert anlegg. Etter kapittel 5 vil nå anleggets klasse som utgangspunkt følge direkte av § 5-2 i forskriften. I tillegg innebærer kapittel 5 at det kan fattes enkeltvedtak om klasse etter § 5-7 på grunnlag av en individuell vurdering.

På denne bakgrunnen vil en virksomhet inngå i KBO etter ny forskrift dersom virksomheten har klassifiserte anlegg etter § 5-2. Videre vil virksomheten inngå i KBO etter første ledd dersom NVE gjennom enkeltvedtak etter § 5-7 fastsetter at et anlegg skal klassifiseres, selv om det i utgangspunktet ikke oppfyller kriteriene for klassifisering etter § 5-2.

3.3.3 Eier eller driver

Med formuleringen ”og som har konsesjon etter *energiloven* §§ 3-1, 3-2 eller 5-1” menes at man må være konsesjonær etter energiloven for å inngå i KBO etter forskriften.

Det er vanlig i kraftforsyningen at den som eier et elektrisk anlegg, også har konsesjonen og driver anlegget. Det er vanlig praksis i NVE at konsesjon for elektriske anlegg og fjernvarmeanlegg kun gis til ett selskap. I de tilfellene hvor eierskapet og driften er skilt, skal konsesjoner etter *energiloven* §§ 3-1, 3-2 og 5-1 innehas av det selskapet som står for driften av anleggene, jf. Ot.prp. nr. 62 (2008-2009).

I de tilfellene hvor det ikke er samsvar mellom eier og driver, er det den som har konsesjonen, som er enhet i KBO etter første ledd. Videre vil det være konsesjonæren som inngår i KBO dersom et anlegg er utleid etter *forskrift om utleie av vannkraftanlegg*.

3.3.4 Andre som kan inngå i KBO etter enkeltvedtak

I noen tilfeller kan en virksomhet som ikke har klassifiserte anlegg, ha mange små anlegg som i sum kan være av vesentlig betydning for energiforsyningen. I andre tilfeller kan det

være selskaper med anlegg som ligger like under grensen for klassifisering, men hvor planlagte utvidelser og utbygging medfører at de vil få klassifiserte anlegg. I slike tilfeller vil NVE kunne vedta at disse virksomhetene skal inngå i KBO. Et tredje eksempel er reguleringsforeningene som har så stor betydning for kraftproduksjonen i et vassdrag, at de bør være med i KBO. Et fjerde eksempel er virksomheter som har ressurser av vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme. Slike virksomheter kan NVE innlemme i KBO etter enkeltvedtak.

NVE kan også anvende bestemmelsen i de tilfellene hvor det vil være naturlig å innlemme en eier av klassifiserte anlegg i KBO, selv om konsesjonen ligger hos en leietaker. Tilsvarende gjelder dersom en leietaker av et vannkraftanlegg etter utleieforskriften skal inngå i KBO. Dersom NVE gjør vedtak om at en virksomhet skal inngå i KBO, kan beslutningen påklages til Olje- og energidepartementet.

3.3.5 Nærmere om industribedrifter

Når det gjelder industribedrifter, viser NVE til drøftingene av klasseinndelingen under § 5-2. Her presiserer vi blant annet at nett- og fjernvarmeanlegg som en industribedrift bruker til egne formål, ikke automatisk klassifiseres. Slike bedrifter vil heller ikke inngå i KBO etter forskrift.

§ 3-4. Ansvar og oppgaver for KBO-enhetene

KBO-enhetene har ansvar for å utføre alle de oppgaver og plikter som følger av energiloven kap. 9 og bestemmelser gitt eller i medhold av denne forskrift, herunder planlegging og håndtering av ekstraordinære situasjoner og gjenoppretting av normal situasjon.

Alle KBO-enheter skal sørge for nødvendig kontakt og samordning med tilgrensende virksomheter og aktuelle kraftforsyningens distriktssjefer.

Beredskapsmyndigheten kan pålegge KBO-enheter eller KBO å utføre oppgaver i medhold av energiloven § 9-1 fjerde ledd.

3.4.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å klargjøre hvilket ansvar og hvilke oppgaver KBO-enhetene har. Pliktene og oppgavene framgår av forskriften som helhet, men bestemmelsen presiserer NVEs mulighet til å pålegge KBO-enhetene ytterligere oppgaver.

3.4.2 Nærmere om KBO-enhetenes ansvar og oppgaver

Denne bestemmelsen beskriver ansvar, oppgaver og plikter for KBO-enhetene. Alle KBO-enheter skal holde NVE og KDS løpende oppdatert med kontaktinformasjon til virksomheten med alle kontaktpersoner, jf § 2-2.

KBO-enheter som har virksomhet i flere KDS-distrikter, må sørge for at det er nødvendig kontakt med KDSene i samtlige distrikt. Det kan oppstå situasjoner hvor KBO-enheten er systemmessig og/eller kommunikasjonsmessig avskåret fra omkringliggende områder. Det betyr at KDS må være kjent med kontaktinformasjon til de lokalt ansvarlige for de enkelte stasjonsanleggene som ligger i distriktet, når disse

anleggene tilhører en KBO-enhet som styrer aktiviteten fra et annet sted (som eksempelvis Statkraft mv.). KBO-enheten er pliktig til å informere KDS om hvem som er stedlig kontaktperson i tillegg til virksomhetens beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator.

Tredje ledd fastsetter at NVE kan gi pålegg om at KBO-enhetene skal utføre oppgaver. Vi kan også gi et slikt pålegg før det er oppstått en ekstraordinær situasjon.

§ 3-5. Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig

KBO-enheter eller KBO kan pålegges oppgaver under beredskap og i krig i samsvar med energiloven § 9-1 femte ledd og etter at beredskapsmyndigheten ved vedtak har konstatert at det anses nødvendig.

Departementet kan under beredskap og krig underlegge energiforsyningen KBO. Energiforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves. Beredskapsmyndigheten kan instruere kraftforsyningens distriktssjefer og KBO-enheter.

I slike situasjoner overtar kraftforsyningens sentrale ledelse (KSL), bestående av beredskapsmyndigheten med deltakelse fra Statnett SF, ledelsen av KBO. Statnett SF skal i slike situasjoner være KSLs utøvende organ for regulering av produksjon, omforming, overføring og fordeling av elektrisk energi.

Statnett SF må innrette sin organisasjon slik at virksomheten har regionale representanter med myndighet til å iverksette pålegg og gjennomføre de tiltak som kreves i en ekstraordinær situasjon, inkludert løpende kontakt med kraftforsyningens distriktssjefer.

3.5.1 Hensikten med bestemmelsen

Denne bestemmelsen beskriver hvilket ansvar, oppgaver og rolle KBO har under beredskap og krig. Det gjelder i de helt spesielle tilfellene hvor Olje- og energidepartementet beslutter at energiforsyningen skal underlegges KBO. I en slik situasjon overtar NVE ansvar og styring over energiforsyningen i Norge.

3.5.2 Nærmere om situasjoner hvor underleggelse er aktuelt

Det er ingen automatikk i at energiforsyningen skal underlegges KBO selv om Olje- og energidepartementet for eksempel beslutter å innføre rasjonering. Olje- og energidepartementet vil gjøre denne vurderingen i hvert enkelt tilfelle, jf *energiloven* § 9-1 femte ledd.

For øvrig viser vi til *energiloven* § 6-2 Rasjonering, som har særlige bestemmelser om hvordan KBO skal brukes, og til *forskrift om planlegging og gjennomføring av rekvisisjon av kraft og tvangsmessige leveringsinnskrenkninger ved kraftrasjonering (rasjoneringsforskriften)*.

I situasjoner hvor KSL blir opprettet, skal KSL holde departementet underrettet om energiforsyningssituasjonen. KSL skal videre sørge for å iverksette nødvendige tiltak i henhold til fullmakt fra departementet.

Når energiforsyningen blir underlagt KBO, overtar KSL ansvaret for landets energiforsyning. Det betyr at alle enhetene som står for produksjon med tilhørende vassdragsanlegg, produksjonsselskap, nettselskap, fjernvarmeselskap og andre enheter i KBO, blir driftsmessig direkte underlagt KSL.

3.5.3 Nærmere om KBO-enhetenes rolle ved beredskap og krig

Når energiforsyningen er underlagt KBO, overtar KSL ledelsen og ansvaret for landets energiforsyning. Alle enheter i KBO plikter å rette seg etter direktiver fra overordnet myndighet innen KBO (det vil si KSL og KDS) og etterkomme kravene fra det tidspunkt de er mottatt. Men ingen KBO-enhet skal avvende eventuelle direktiv fra KSL eller KDS, men gjøre det som er nødvendig for å opprettholde normal drift så lenge som mulig.

§ 3-6. Ansvar og oppgaver for kraftforsyningens distriktssjefer

Beredskapsmyndigheten beslutter inndeling av distrikter og utpeker kraftforsyningens distriktssjefer med stedfortredere.

Kraftforsyningens distriktssjefer (KDS) skal bidra til å tilrettelegge for hensiktsmessig samarbeid om forebygging og håndtering av ekstraordinære situasjoner. Oppgaver for KDS kan reguleres gjennom avtaler mellom beredskapsmyndigheten og den person som er utpekt som KDS og i årlige forventningsbrev. Fullmakt til vedtak kan delegeres fra beredskapsmyndigheten til KDS.

3.6.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å gjøre det tydelig hvem som utpeker KDS, hvilken myndighet KDS har og KDS sin rolle regionalt. KDS er KBOs og NVE sine regionale representanter og skal være bindeledd mellom KBO-enhetene og NVE og KSL.

3.6.2 Nærmere om oppnevning av KDS

KDSene med stedfortredere utpekes av NVE. De skal som hovedregel utpekes fra en enhet i KBO som vanligvis driver det regionale nettet innenfor et større område (distrikt). Normalt legges KDS-funksjonen til det selskapet som ivaretar myndighetspålagte energiutredninger i området (jf *forskrift om energiutredninger*). Beredskapsmyndigheten kan fravike denne hovedregelen.

Innenfor det geografiske ansvarsområdet til en KDS vil det være ulike former for energiselskap.

NVE utarbeider årlige forventningsbrev til KDSene. KDSene skal ha oversikt over de viktigste beredskapsmessige utfordringene innenfor sine distrikter, tilrettelegge for samarbeid og samordning mellom KBO-enhetene og bidra med råd og veiledning om sikringstiltak og beredskap.

KDSene er energiforsyningens regionale representanter når de i henhold til gjeldende lov og forskrifter utøver sitt ansvar og sine oppgaver. KDS representerer energiforsyningen i fylkesmannens beredskapsråd.

3.6.3 Nærmere om bestemmelsen

Første ledd beskriver NVEs rett til å dele inn KDS-distriktene og utpeke KDSer med stedfortreder. Det skjer ved en formell oppnevning som NVE gjør kjent ovenfor KBO-enhetene og fylkesmannen. Ved utnevningen inngår NVE en gjensidig oppsigelig avtale med KDSen der varigheten av engasjementet og oppgavene er nærmere beskrevet.

Andre ledd i bestemmelsen beskriver ansvar og oppgaver for kraftforsyningens distriktssjefer. KDSene får årlig et forventningsbrev fra NVE som beskriver oppgavene som de skal utføre.

NVE kan gi fullmakt til å fatte vedtak til KDSene, uavhengig om det er krisesituasjoner. KDSen har i slike situasjoner myndighet til å fatte vedtak overfor alle enheter i KBO innenfor sitt eget distrikt på vegne av NVE. Slike fullmakter skal være dokumenterbare.

KDSene skal være bindeledd mellom enheter i KBO og fylkesmannen på regionalt nivå, og inngå i fylkesmannens beredskapsråd. NVE forventer at KBO-enhetene i et distrikt møter når KDS innkaller til samarbeidsmøter innenfor forskriftens virkeområde. Alle enhetene i KBO plikter å rapportere til KDS i forbindelse med ekstraordinære hendelser der KDS er satt til å koordinere løpende rapportering. Og KDS plikter i sitt beredskapsplanverk å ha kapasitet til å ivareta en koordinerende rapporteringsrolle. Den enkelte KDS skal også samarbeide med andre KDSer der regionene henger sammen forsyningssikkerhetsmessig.

§ 3-7. Fritaksordninger

Etter søknad fra en KBO-enhet kan personell som er viktig for å opprettholde driften av energiforsyningen i krig, få utsettelse eller fritak for fremmøte i Forsvaret ved mobilisering. Etter søknad fra en KBO-enhet kan dette personellet også få fritak for tjeneste i sivilforsvaret og politireserven. Personell i KBO som er gitt utsettelse eller fritak for annen beredskapstjeneste får tjenesteplikt i KBO.

3.7.1 Hensikten med bestemmelsen

Bestemmelsen er en hjemmel som sikrer bemanning i energiforsyningen ved mobilisering og krig, siden annet regelverk gir hjemmel til å hente inn personell til blant annet Forsvaret. Denne hjemmelen om å søke fritak gjelder for alle enhetene i KBO.

3.7.2 Fritak for/Utsettelse med frammøte i Forsvaret ved mobilisering

Forsvaret kan etter melding/søknad gi personell som er nødvendig for driften av energiforsyningen i krig fritak for eller utsatt frammøte i tilfeller der Forsvaret mobiliserer. En betingelse for å kunne være med på "fritaksordningen", er at selskapet har utarbeidet et beredskapsplanverk hvor vedkommendes rolle i beredskapsorganisasjonen framgår, og en plan for hvordan arbeidskraftbehovet ved krigsberedskap skal dekkes.

Forutsetningene for at det gis fritak for frammøte i Forsvaret er at:

- Arbeidstakeren dekker en kritisk funksjon i virksomheten,
- Arbeidstakeren har fullført førstegangstjenesten og

- Arbeidstakeren er disponert eller planlagt disponert i Forsvarets styrker, Heimevernet inkludert, har fått brev om nytilføring til Heimevernet eller er innkalt til repetisjons-/hjelpetjeneste.

Regelverket for fritaksordningen i Forsvaret er under endring, og nytt regelverk skal i følge Forsvaret innføres i 2013. Forsvarsdepartementet har gjort det gjeldende regelverket "sovende" inntil nytt regelverk blir innført. For nærmere informasjon henviser NVE til www.forsvaret.no og <http://forsvaret.no/verneplikt/etter-forstegangstjenesten/Sider/fritaksordninga.aspx>.

Skjema for å søke om fritak finnes som vedlegg 8 til veiledningen. Dersom en søknad blir avslått, kan KBO-enheten klage på avgjørelsen. Skjema for klage er vedlegg 9 til veiledningen.

3.7.3 Fritak for tjeneste i Sivildforsvaret og Politireserven

I henhold til kgl. Res. av 24. mai 1985 kan nøkkelpersonell i kraftforsyningen fritas for tjeneste i Sivildforsvaret. Ordningen er ment å gi fritak for det personellet som er viktigst og vanskeligst å erstatte innen drift, verksted, lager og merkantil avdeling.

Det enkelte energiselskapet skal sende skriftlig melding til vedkommende sivilforsvarskrets om hvilket nøkkelpersonell som ønskes fritatt for tjeneste i Sivildforsvaret. Meldingen skal gi opplysninger om navn, fødselsnummer (11 siffer) og stilling i selskapets beredskapsorganisasjon. Ved fratredelse i fritaksberettiget stilling, plikter både den enkelte og selskapet å underrette sivilforsvarskretsen om det.

Nøkkelpersonell i kraftforsyningen kan på liknende måte søkes fritatt for tjeneste i Politireserven. Søknaden sendes vedkommende politidistrikt.

Kapittel 4. Ressurser og reparasjonsberedskap

Kapitlet beskriver beredskapen som den enkelte KBO-enhet må ha, og hvilke krav som må oppfylles for at reparasjonsberedskapen er tilfredsstillende når behovet oppstår. Kapitlet stiller både krav til organisering, kompetanse og ressurser.

Kravene skal sikre at den enkelte KBO-enheten har nødvendige ressurser raskt tilgjengelig i ekstraordinære situasjoner. Bestemmelsene krever at enhetene har tilgang til tilstrekkelig antall personell til å drifte energiforsyningen i ekstraordinære situasjoner og til å gjenopprette forsyningen ved behov. I tillegg må personellet ha den rette kompetansen til å utføre oppgavene sikkert og effektivt. Det skal alltid være sikre arbeidsforhold for mannskap i henhold til arbeidsmiljølovens bestemmelser, *forskrift om sikkerhet ved arbeid og drift av elektriske anlegg*, og etter *forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff, samt utstyr og anlegg som benyttes ved håndteringen*.

Enheten må videre ha tilgang til nødvendige komponenter og utstyr til gjenoppretting. Dette inkluderer anleggsdeler, verktøy, transportutstyr, sambandsutstyr og annet relevant utstyr.

§ 4-1. Reparasjonsberedskap

Alle KBO-enheter skal planlegge for og etablere en organisasjon med nødvendig personell, kompetanse, utholdenhet og ressurser til å holde driften gående, gjenopprette funksjon og gjennomføre oppgaver som kreves under alle ekstraordinære situasjoner på en sikker og effektiv måte.

Reparasjonsberedskapen skal dimensjoneres etter stedlige forhold og anleggenes tilstand og klasse. Så langt som det er samfunnsmessig rasjonelt, skal hensynet til liv og helse og annen samfunnskritisk virksomhet prioriteres ved gjenoppretting av funksjon.

4.1.1 Hensikten med bestemmelsen

Hensikten er å sikre drift og rask gjenoppretting i ekstraordinære situasjoner.

4.1.2 Nærmere om reparasjonsberedskapen

KBO-enhetene skal ha en reparasjonsberedskap som står i forhold til alle former for ytre påkjenninger og risiko for andre ekstraordinære hendelser. I tillegg må reparasjonsberedskapen dimensjoneres etter hvilken type anlegg virksomhetene har, som for eksempel sjøkabler og fjordspenn, anleggets klasse og samfunnskritiske betydning. Dette inkluderer forsyning til eventuelle skjermingsverdige objekter etter sikkerhetslovgivningen. Se også § 2-5. *Beredskapsplanlegging* og kravet til samordning med berørte myndigheter og andre relevante virksomheter.

Videre stilles det krav til utholdenhet. For å være utholdende, må enheten ha en beredskap for langvarige og omfattende hendelser, og med flere samtidige hendelser. Et eksempel kan være rasjonering med uvanlig mange koblinger i nettet og feil på mange komponenter.

KBO-enhetene skal ha oversikt over virksomheter med betydning for liv og helse, og annen samfunnskritisk virksomhet i sitt område, og ha en god dialog med disse i det løpende beredskapsarbeidet, og legge dette til grunn i sitt beredskapsplanverk.

Det forventes at energiforsyningen gjenopprettes også etter omfattende ødeleggelser uansett hva som er årsaken. Enhetene må derfor analysere hvilke hendelser som skal være dimensjonerende for reparasjonsberedskapen.

Prioriteringskriteriene for gjenoppretting skal være i samsvar med det som er angitt i *forskrift om planlegging og gjennomføring av rekvisisjon av kraft og tvangsmessige leveringsinnskrenkninger ved kraftrasjonering (rasjoneringsforskriften) § 9,*

- a) liv og helse;
- b) vitale samfunnsinteresser innenfor administrasjon og forvaltning, informasjon, sikkerhet, infrastruktur, forsyninger mv.;
- c) næringsliv og berørte økonomiske interesser.

En særlig vital samfunnsinteresse vil være eventuelle skjermingsverdige objekter etter sikkerhetslovgivningen. Feilretting kan ikke alltid baseres på karakteristika ved kundene, men på hva som er mulig å oppnå i feilsituasjonen. Selv om samfunnskritiske virksomheter kan ha krav til egenberedskap i form av nødstrøm, er det likevel en forventning om at de skal få strømmen tilbake så snart som mulig. Uansett vil alltid hensynet til liv og helse ha førsteprioritet.

§ 4-2. Kompetanse og personell

Alle KBO-enheter skal ha personell med nødvendig kompetanse som kreves for kunne håndtere ekstraordinære situasjoner på en sikker og effektiv måte.

Alle KBO-enheter skal dekke dette personellbehovet og ha tilgang på personell for å forsterke kapasiteten og holde driften gående i ekstraordinære situasjoner.

For å dekke kravet til kompetanse og personell skal det foreligge en plan som angir kompetansebehovet, og som omfatter eget og innleid personell.

4.2.1 Hensikten med bestemmelsen

Håndtering av ekstraordinære situasjoner på en sikker og effektiv måte, betyr sikkerhet for at personell ikke skades, at personellet har den kompetansen som er nødvendig for oppgaven, og at metoder og utstyr er de rette og fungerer effektivt.

4.2.2 Nærmere om kompetanse

Enheten må ha kompetanse for å sikre at alle krav i beredskapsforskriften blir ivaretatt, slik at enheten kan håndtere alle ekstraordinære situasjoner som hindrer energiforsyningen. Enheten bør ta hensyn til at kritisk viktige medarbeidere kan være forhindret fra å stille opp i en ekstraordinær situasjon.

KBO-enheten skal selv ha sentral kompetanse for å håndtere ekstraordinære situasjoner. Enheten kan velge om ytterligere tilgang på kompetanse sikres gjennom eget personell, innleid personell eller gjennom samarbeidsavtaler. Dette forutsetter at enheten utfører oppgavene sikkert og effektivt, og følger øvrig lovgivning som setter krav til kompetanse

og bemanning. Legg merke til at kompetansekravet blant annet omfatter så ulike forhold som:

- Kriseledelse.
- Sikring og drift av anlegg i ekstraordinære situasjoner, herunder produksjon, nett, fjernvarme, driftskontrollsystemer og samband.
- Gjenoppretting og reparasjon.
- Krisekommunikasjon.

I en beredskapssituasjon skal enheten ha sikker tilgang på fagfolk som har erfaring i å betjene anleggene ved lokal styring.

Leder for virksomheten (daglig leder eller tilsvarende), beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator vil kunne utgjøre kjernekompetansen for styring av enheten gjennom ekstraordinære situasjoner. Forventningene NVE har til disse funksjonene er nærmere beskrevet i veiledningen til § 2-2. Krav til kompetanse hos driftssentralpersonell framgår av § 7-9 og er nærmere beskrevet i veiledningen til denne bestemmelsen.

4.2.3 Nærmere om personell

Det anbefales å lage en prioritert oversikt over hvilke funksjoner som alltid må ivaretas for å holde driften gående, og spesielt de som er viktige i ekstraordinære situasjoner. Personellplanen skal inkludere de personene som har denne kompetansen. Behovet for personell kan omfatte blant annet kriseledelse, reparasjon, gjenoppretting av driften og å holde driftskontrollfunksjoner i gang.

4.2.3.1 Personellbehovet i ekstraordinære situasjoner

Det skal foreligge planer for å dekke personellbehovet til de ulike funksjonene i ekstraordinære situasjoner. Planene bør bygge på oversikten over hvilke funksjoner som alltid skal ivaretas, og inneholde:

- Oversikt over tilgjengelig personell.
- Om enheten til enhver tid har nok personell til å dekke nødvendige funksjoner i en ekstraordinær situasjon.
- Personellets funksjon og eventuell spesialkompetanse.
- Nødvendig kontaktinformasjon.

Personellplanene bør oppdateres minst én gang i året. I den utstrekning enheten er avhengig av personell utenfor egen virksomhet, må den utarbeide tilsvarende personellplaner for disse. Enheten må inngå robuste avtaler om prioritet, slik at enheten sikres det innleide personellet i ekstraordinære situasjoner. *Forskrift om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften)* gjelder drift i normalsituasjoner, mens beredskapsforskriften gjelder drift og gjenoppretting i ekstraordinære situasjoner. Den bemanningen enheten må ha etter *kompetanseforskriften*, vil naturlig inngå i de ressursene som trengs i en ekstraordinær situasjon. Men personellbehovet kan bli langt større i en slik situasjon. Det må skaffes sikker tilgang til personell som ikke er en del av egen grunnbemanning ved avtaler. Slike avtaler kan inngås med andre KBO-enheter, eller driftsselskaper, entreprenørselskaper og leverandører.

§ 4-3. Drift i ekstraordinære situasjoner og gjenoppretting av funksjon

Alle KBO-enheter skal i ekstraordinære situasjoner drive de anlegg og den del av energiforsyningen enheten har ansvaret for, herunder driftskontrollfunksjoner, og gjenopprette nødvendige funksjoner i og etter ekstraordinære situasjoner.

4.3.1 Hensikten med bestemmelsen

Dette er et krav om å opprettholde energiforsyningen og drive anleggene med en høy grad av sikkerhet også i ekstraordinære situasjoner. Driftskontrollfunksjonene har stor betydning for drift og gjenoppretting i ekstraordinære situasjoner. Det er derfor et eksplisitt krav om at driftskontrollfunksjonene skal drives og gjenoprettes i ekstraordinære situasjoner.

4.3.2 Drift og gjenoppretting i ekstraordinære situasjoner

Enheten forutsettes å ha dokumentasjon om energiforsyningsanlegg, energisystemet, prioriterte kunder, utkoblbar last, koblingsbilder og flaskehalser. Enheten kan bruke denne dokumentasjonen i en ekstraordinær situasjon for å gi sikrere gjenoppretting og for å starte gjenopprettingen i en prioritert rekkefølge. Ved feil i nettet kan det oppstå flaskehalser på nye steder.

Enheten skal:

- Ha beredskapsplaner for drift og gjenoppretting med alle nødvendige ressurser under ekstraordinære situasjoner.
- Sørge for sikre arbeidsforhold for mannskap i henhold til *arbeidsmiljølovens* bestemmelser, *forskrift om sikkerhet ved arbeid og drift av elektriske anlegg*, *forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff*, samt *utstyr og anlegg som benyttes ved håndteringen* § 7 Kompetanse, siste ledd.
- Ta hensyn til at spesielle forhold – som ekstremvær – kan forsinke gjenopprettingen, men at gjenopprettingen likevel skal skje.
- I beredskapsplanene ta hensyn til påregnelige vansker ved gjenoppretting, slik som for eksempel stengte veger.

Enheten må ha tilstrekkelig med kompetent driftspersonell, se § 4-2 Kompetanse og personell. Enheten må:

- Sikre at den har så mange personer tilgjengelig at det blir mulig å greie seg gjennom langvarige situasjoner, eksempelvis en rasjonerings situasjon med sonevis utkobling i flere uker.
- Kunne håndtere ekstraordinært press over lang tid, for eksempel dersom det oppstår flere driftsfeil samtidig.
- Ta høyde for at det kan oppstå flere samtidige hendelser.

Eksempel på samtidige hendelser:

Uvær slår ut flere forsyningslinjer og ekomtjenester.

Ras rammer en kraftlinje samtidig med svikt i driftskontrollsystemet.

Teknisk svikt på flere forsyningslinjer til samme område.

Stort rørbrudd og sterk kulde.

Enheten bør også ta høyde for at én eller flere hendelser samtidig kan ramme flere KBO-enheter innenfor samme geografiske område. Dette er et hensyn som særlig bør ivaretas når det gjelder tilgang på personell.

4.3.3 Gjenoppretting av funksjon i og etter ekstraordinære situasjoner

KBO-enhetene skal sørge for at energiforsyningen har korte gjenopprettingstider også i ekstraordinære situasjoner. Det som skal gjenopprettes, er funksjon i anlegg og komponenter i alle typer anlegg – kraftstasjoner, fjernvarmeanlegg, transformatorstasjoner, koblingsanlegg, ledningsanlegg og driftskontrollsystemer. Det betyr at både anleggets funksjonalitet skal gjenopprettes og at ødelagte komponenter skal repareres eller erstattes. Anleggets funksjonalitet skal gjenopprettes uten ugrunnet opphold eller så raskt som fysisk mulig, avhengig av anleggets klasse, i henhold til §§ 5-4 – 5-6 Sikringstiltak for klassene 1, 2 og 3.

4.3.4 Reparasjonsberedskap i driftskontrollsystemer

For driftskontrollsystemets mest vitale og mest utsatte enkeltkomponenter skal det etableres særskilt reparasjonsberedskap, enten i egen enhet eller kontraktfestet hos eksterne leverandører.

4.3.5 Reparasjonsberedskap i sentral- og regionalnettet med tilgrensende kraftstasjoner

Forventninger til god reparasjonsberedskap ble identifisert i prosjektet Reparasjonsberedskap, som hadde bransjedeltakelse. Disse forventningene har vært på høring i bransjen. NVE har her valgt å videreføre resultatene fra prosjektet (som ble brukt i veiledningen til BfK fra 2011) for å synliggjøre hva som er rimelige forventninger til KBO-enhetene. Videre vil vi henviser til mer spesifikke krav for klassifiserte anlegg under kapittel 5 og vedlegg 1 til 3 (til bfe).

For å oppnå god reparasjonsberedskap må alle forhold listet opp nedenfor være vurdert. Ressursene må være tilstrekkelige og tilgjengelige i ekstraordinære situasjoner. Hver enkelt KBO-enhet bør på forhånd gjennomføre en egen vurdering og bestemme akseptabel responstid for startfasen etter en uønsket hendelse og dokumentere dette i beredskapsplanen. Uakseptable responstider og reparasjonstider kan identifiseres gjennom dette arbeidet. Enheten må treffe risikoreduserende tiltak når det viser seg nødvendig. Tiltakene skal være forberedt og innøvd.

4.3.5.1 Personressurser, kapasitet over tid

Enheten må sikre seg tilstrekkelig kompetanse, herunder:

- Egne ansatte og ansatte i samme konsern.
- Innleide (beredskapsavtale og opptrappingsplan med entreprenører).
- Samarbeidsavtaler (med andre KBO-enheter).
- Kort responstid.
- Utholdenhet.

4.3.5.2 Kompetanse

Enheten skal sørge for egen kompetanse og kompetanse hos leverandører/entreprenører i forhold til å løse oppgaver knyttet til:

- Oljekabel (fases ut over tid, men viktig for mange anleggseiere).
- Kryssbundet polyetylenkabel (PEX) (krever spesialkompetanse ved høye spenninger).
- Sjøkabel – olje og PEX.
- Transformatorer (spisskompetanse finnes hos leverandører, men noen vurderinger må gjøres i enheten og krever funksjonskompetanse).
- Gassisolerte apparatanlegg (SF₆-anlegg) (132 kV mer standard, 300-400 kV skreddersøm). Det er en egen brukergruppe med fagkompetanse og oversikt over beredskapsutstyr. Kompetanse for øvrig finnes hos leverandører.
- Effektbrytere.
- Linjemontasje (på grunn av radialer i regionalnett. Ressurser forventes å finnes hos entreprenører).
- Driftskontrollsystemer (behov for overordnet kompetanse i enheten).
- Relévern og måletransformatorer (viktig for å kunne etablere provisorisk drift).

4.3.5.3 Forberedte tiltak

Enheten må forberede:

- Tiltak for spesielle / samtidige / ekstraordinære hendelser.
- Beredskapsplaner for ekstraordinære hendelser.
- Øvelser.
- Tiltak for nødløsninger / provisorier, ”verktøykasse” med alternative løsninger. (Eksempelvis forbikobling av brytere og måletransformatorer, omstilling av vern).
- Arbeid i nettet for å kunne gjenopprette eller koble om når feil oppstår.
- Produksjon med innmating i nettet.
- Plan for å ta imot bistand.

4.3.5.4 Kriseledelse

Enheten skal ha opplegg for:

- Krisestab med oversikt, overordnede prioriteringer og beslutninger.
- Risikovurderinger i forhold til aktuell hendelse (mørke, storm, rasfare, flom, is eller liknende).
- Helse, miljø og sikkerhet.
- Mediehåndtering.

4.3.5.5 Administrativt

Enheten må sørge for:

- Plan for å ta imot bistand, og tolk for eventuelt utenlandsk mannskap.
- Kundehåndtering (herunder sentralbord).
- Rapportering.
- Overnatting, mat og drikke.

4.3.5.6 Produksjon

Enheten må vurdere:

- Lokal innmating.
- Produksjon i samråd med Statnett (effekt) eller lokalt nettselskap (jf *systemansvarsforskriften* og *rasjoneringsforskriften*).

4.3.5.7 Forventninger til responstid

For å oppnå god beredskap er det forventninger til responstider:

- Forventet tid til oppdagelse av vesentlige feil i alle systemer av betydning for drift og sikkerhet, raskt/straks (jf klasse – se kapittel 5).
- Forventet tid fra feilen har skjedd til provisorisk forsyning kan gjenopprettes, opp til 1-2 døgn.
- Tilgang på alle nødvendige ressurser.

Tidene nedenfor bør være mulig å oppnå for alle feilsituasjoner i sentral- og regionalnettet og i alle klasser av anlegg. Når alle viktige anlegg og et stort antall kunder er berørt, forventer NVE at KBO-enheten skal kunne gjenopprette forsyningen innenfor nedre del av de angitte tidene.

Ved redundans i systemet eller når $N \div 1$ -kriteriet er oppfylt, skal forsyningen gjenopprettes øyeblikkelig og automatisk eller ved kobling. Når systemet ikke har redundans (er forsynt radielt), skal enheten legge stor vekt på å ha forberedt provisorisk forsyning. I enkelte feiltilfeller hvor det i utgangspunktet er bygget med redundans, kan likevel funksjonaliteten rammes hvis flere redundante komponenter rammes.

Prosjektet Reparasjonsberedskap i sentral- og regionalnettet og tilknyttede kraftstasjoner har skissert responstidene skissert for ulike situasjoner, avhengig av driftskontrollsystemets klasse, om $N \div 1$ -kriteriet er oppfylt, om kunder rammes, omfang, og delt opp etter type anlegg og fasene i omkobling og reparasjon.

Skisse til responstider, basert på Prosjektet Reparasjonsberedskap i sentral- og regionalnettet og tilknyttede kraftstasjoner:

Klasse 3 driftskontroll - omkobling er mulig:

- Oppdage hendelsen straks i driftssentral/ driftskontrollsystem, jf § 5-6, vedlegg 3 Særlige krav til sikring for anlegg i klasse 3.
- Vurdere situasjonen og foreta omkobling så raskt som fysisk mulig for å gjenopprette forsyningen (anslagsvis 1 minutt til 1 time).

- I stasjonsanlegg kan det være nødvendig å sende ut mannskaper så raskt som fysisk mulig for å se omfanget/ hvilken del av stasjonsanlegget som er ”friskt” før innkobling foretas, ½ - 1 time.
- Videre reaksjonsmønster i henhold til beredskapsplan, jf § 2-5 med angitte beredskapstiltak og responstider.
- Kun unntaksvis skal kundene være uten strøm i mer enn 1-2 timer ved slike feil i sentral- og regionalnettet. Hvis dette ikke er tilfelle, se feil som medfører avbrudd i forsyningen, under.
- Etter gjennomført startfase kan det ta dager til måneder for å gjenopprette status som før feilen oppstod – se nedenfor for reparasjon.

Klasse 2 driftskontroll - omkobling er mulig:

- Oppdage hendelsen raskt i driftssentral/driftskontrollsystem, (anslagsvis 1 til 15 minutter), jf § 5-5 Sikringstiltak for klasse 2.
- Vurdere hendelsen og iverksette innledende tiltak uten ugrunnet opphold, (anslagsvis 10 til 15 minutter).
- Videre reaksjonsmønster i henhold til beredskapsplan, jf § 2-5 med angitte beredskapstiltak og responstider.

Etter gjennomført startfase kan det ta dager til måneder for å gjenopprette status som før feilen oppstod – se nedenfor for reparasjon.

Klasse 2 og 3 driftskontroll - Feil som medfører avbrudd i forsyningen til kunder:

- Oppdage og vurdere hendelsen – se over.
- Bestemme innledende tiltak, (anslagsvis 5 til 15 minutter).
- Innkalle mannskap for kriseledelse, lokalisering av feil med mer, (anslagsvis 15 minutter).
- Mannskap klar for utrykking, (anslagsvis 15 minutter til 2 timer).
- Kartlegge og vurdere hendelsen i detalj, (fra timer til døgn, avhengig av tilgjengelighet, værforhold, risiko ved befaring og andre forhold på stedet).
- Reparasjon av ødelagt anlegg eller komponent, (fra timer til måneder).
- Provisorisk løsning etableres for å gjenopprette forsyningen, (anslagsvis 4 timer til 1 døgn).
- Gjenopprette forsyningen provisorisk fra en helt ødelagt transformatorstasjon, 3 til 4 døgn.

Avbrudd med stort omfang:

- Innledende faser som over.
- Etablere krisestab.

- Sende ut mannskaper for å se omfanget og vurdere tiltak, (anslagsvis ½ til 2 timer avhengig av vær).
- Innkalle beredskapsressurser (materiell og mannskaper).
- Iverksette eventuelle midlertidige løsninger (kabler på bakken, provisoriske koblingsanlegg).

Reparasjonsfasen:

- Begynne reparasjoner så snart som praktisk mulig.
- Beredskapsmaster settes opp, kabler skjøtes, transformatorer flyttes og liknende.
- Til skjøting av oljekabler og andre situasjoner der det kreves tilgang på spesialkompetanse, må det legges ekstra vekt på forberedte tiltak.
- Reparasjon fullført og provisorisk løsning avvikles, full normal funksjonalitet, (anslagsvis minutter til døgn; prøvekoblinger, stille reléer, forsiktig opplasting).

Produksjonsanlegg i klasse 2 og 3:

- Oppdage hendelsen raskt/straks i driftskontrollsystemet.
- Vurdere situasjonen, iverksette innledende tiltak uten ugrunnet opphold/så raskt som fysisk mulig.
- Foreta omkobling for å gjenopprette mest mulig av forsyningen (1 minutt til 1 time).
- Det kan være nødvendig å sende inn mannskaper for å se på omfanget og hvilke deler av anlegget som er ”friskt” for innkobling (½ til 3 timer).
- Gjøre beslutninger om videre tiltak, neste arbeidsdag.
- Innkalle relevante beredskapsressurser (materiell og mannskaper).
- Igangsette reparasjonsarbeider.
- Deretter kan det ta fra dager til måneder for å gjenopprette status som før feilen oppstod.

4.3.6 Reparasjonsberedskap for distribusjonsnett og fjernvarme

Krav til gjenoppretting av funksjon gjelder alle nettnivåer og klasser, og både for produksjon og distribusjon av elektrisitet og fjernvarme. Feil langt ute i nettet, nær forbrukerne, fører som regel til avbrudd i forsyningen. Ofte finnes det ikke omkoblingsmuligheter. Det er derfor av like stor betydning å:

- Oppdage feil raskt.
- Gjøre innledende vurderinger.
- Lokalisere feilsted.
- Sende ut mannskap for å starte med reparasjoner uten ugrunnet opphold.

- Iverksette midlertidige løsninger hvis avbrudd kan forventes å vare i mer enn noen timer.

Det bør legges til grunn forventninger til responstid som for sentral- og regionalnettet med kraftstasjoner beskrevet ovenfor. I tillegg må det i distribusjonsnettet legges stor vekt på aggregatdrift inntil feil er reparert, for at samfunnsviktige funksjoner kan opprettholdes. NVE presiserer at alle kunder som er kritisk avhengige av kontinuerlig strømforsyning, selv har ansvar for å sikre egen nødstrøm.

4.3.7 Reparasjonsberedskap for sjøkabelanlegg

Kraftforsyningen i Norge har et stort antall sjøkabelanlegg på alle nettnivåer. Det er anslagsvis 150 sjøkabelanlegg i sentral- og regionalnettet og rundt 2 000 i distribusjonsnettet.

Mange av anleggene kjennetegnes ved at de kan ha stor betydning for forsyningen på alle nettnivåer. Det kreves spesialkompetanse for å reparere dem, og anleggene må overvåkes nøye fordi de kan være spesielt utsatt for å bli påført skade.

For å oppnå god sikkerhet ved anleggene er tiltak i innkjøps- og konstruksjonsfasen, så vel som i daglig drift og ved feilretting av stor betydning. Veiledningen beskriver derfor alle disse forholdene. Veiledningen beskriver bare et minimumsnivå for god beredskap. Egne analyser av sårbarhet og dimensjonering av beredskap vil kunne føre til behov for et høyere nivå.

For kabler med olje- og papirisolasjon er feilretting og reparasjon krevende, og tilgangen på kompetanse er begrenset. Kabelteknologi med bruk av plastisolering (PEX) gir enklere kabelkonstruksjoner som ikke er like kompliserte å reparere.

Det er etablert en gruppe *Sjøkabelberedskap* som er tilknyttet *eBeredskap*. *Sjøkabelberedskap* har forhandlet fram landsdekkende beredskapsavtaler med to rederier. Medlemmene må selv skaffe seg skjøtekompetanse.

Ansvar for å ha tilstrekkelig kompetanse og beredskap ligger uansett hos den som eier eller driver anlegget.

4.3.7.1 Sjøkabelberedskap i sentral- og regionalnettet

Alle eiere av sjøkabelanlegg i sentral- og regionalnettet skal ha tilgang på kompetanse, reparasjonsmateriell, reservedeler og transportmidler slik at reparasjon eller utskifting av kabelanlegget kan påbegynnes og utføres uten unødig opphold. Hvis enheten ikke har dette selv, må den inngå skriftlig avtale som sikrer slik tilgang. Flere sjøkabeleiere kan gå sammen om å inngå slike avtaler. Eiere som har sjøkabelanlegg over 1 kilometer, bør være med i gruppen *Sjøkabelberedskap*.

Kabelanlegg bør legges ned på sjøbunnen slik at frispenn unngås. Tilfeldige feil som følge av ytre påkjenning kan medføre skade på flere faser. Derfor anbefaler NVE at virksomheten vurderer en avstand mellom enkeltledere på minst 150 meter. Legging av reservelengder må vurderes for svært viktige anlegg. Nye kabelanlegg bør vurderes lagt i god avstand fra eksisterende anlegg.

Tilgang til følgende ressurser må sikres:

- Fartøy med nødvendig utstyr og mannskap.

- Biler for kabeltransport.
- Krankapasitet.
- Skjøtekompetanse.
- Reserverlengder av kabel for innskjøting eller hele lengder for erstatning.
- Endemuffer, skjøtemuffer og overgangsmuffer for å dekke feil på mer enn 1 fase.
- Nødvendig reparasjonsmateriell, verktøy og utstyr.
- Festemateriell for landtak.
- Oversikt over reservedeler og reparasjonsutstyr og system for å holde dette i forsvarlig stand.
- Oppdaterte trasékart og inntegning av ankringsforbudssone i sjøkartet.
 - Det bør vurderes en ankringsforbudssone som dekker hele trasébredden og et område på minst 250 meter på hver side.
- Utstyr og kompetanse for feilsøking og feilstedlokalisering.
- Alternative planer for drift av nettet inntil anlegget igjen er fullt funksjonsdyktig.
- Sjekkliste for håndtering av kabelfeil for hvert enkelt kabelanlegg.
- System for å holde kabelanlegget i forsvarlig stand slik at det driftsmessig er tilgjengelig:
 - Kontinuerlig overvåking og logging av oljetrykk og spenning og overføring av alarmer til døgnbemannet driftssentral.
 - Kvartalsvis kontroll/ettersyn av oljetrykksanlegg.
 - Årlig ettersyn av landtak, skilt, overspenningsavledere, endemuffer og muffehus, samt elektrodelen av katodisk beskyttelse.
 - Regelmessig oljeanalyse i henhold til gjeldende norm, for tiden NEK 240-2:2009 Isoleroljer – Kvalitative krav, overvåkning og vedlikehold -- Del 2: Kabelanlegg for kraftforsyning.
 - Minst hvert 4. år ROV/dykker-inspeksjon av kabel, sjødelen av katodisk beskyttelse og avlastning ned til 50 meter dybde og/eller 500 meter fra landtaket.
 - Minst hvert 10. år inspeksjon av hele kabellengden med oppdatering av trasékart.
 - Øvrige forhold som kabelleverandøren har angitt.
- Kompetanseutvikling.
 - Alle eiere av sjøkabelanlegg må sørge for egen kompetanseutvikling innen fagfeltet.
 - Informere *Sjøkabelberedskap* eller andre eiere av sjøkabler om kabelfeil og erfaringer fra reparasjoner.
- For hvert enkelt sjøkabelanlegg bør følgende dokumenteres og opplysningene være lett tilgjengelige:
 - Kontaktpersoner.
 - Handlingsplan ved kabelfeil.
 - Feilsøking og reparasjon.
 - Juridiske forhold og miljøspørsmål.
 - Informasjonshåndtering og varsling.
 - Avtaler og kontrakter om bistand.
 - Forsikringer.

- o Anleggsdata.
- o Reservedeler og reparasjonsutstyr.
- o Krav til reparasjonsfartøy og spesifikasjon for innleie.
- o Adresseliste over relevante leverandører, organisasjoner og myndigheter.
- o Oversikt over andre rør- og kabelinstallasjoner med eiere i området for kabelanlegget.

4.3.7.2 Sjøkabelberedskap i distribusjonsnettet

Eierne har ofte sikker tilgang til alle ressurser som trengs, eller de kan få tilstrekkelig tilgang hos andre everk eller entreprenører i området. I distribusjonsnettet benyttes ofte en enklere teknologi med mer standardisert og tilgjengelig materiell.

Det stilles ikke krav om at det skal være inngått beredskapsavtaler i de tilfellene der kabelanleggene er korte, dybdene ikke er store og driften kan opprettholdes med aggregat. KBO-enheten skal imidlertid kunne dokumentere planer for å reparere eller skifte ut anlegget ved havari, og hvordan de vil opprettholde strømforsyningen ved feil på kabelanlegget.

Veiledningen til sjøkabelberedskap i sentral- og regionalnettet gjelder også for spesielle og viktige sjøkabelanlegg i distribusjonsnettet. Dette gjelder spesielt ved mangel på redundans, og ved store kabellengder og store dyp. Dette gjelder uavhengig av mulighet for aggregatdrift.

Eiere som har sjøkabelanlegg over 1 kilometer med spenning over 1 kV bør være med i *Sjøkabelberedskap*.

§ 4-4. Materiell og utstyr

Alle KBO-enheter skal ha rask og sikker tilgang til reservemateriell og utstyr som trengs for å opprettholde energiforsyningen i ekstraordinære situasjoner, og for å gjenopprette funksjon.

Med reservemateriell menes materiell som kan erstatte komponenter som er nødvendige for drift av anlegg.

Med utstyr menes verktøy, maskiner, reparasjonsmateriell, komponenter til driftskontrollsystemet og annet som er nødvendig for å foreta reparasjoner, gjenoppretting eller om nødvendig iverksette midlertidige tiltak.

Ressursbehovet kan dekkes ved at KBO-enheten enten har dette selv, eller sikrer tilgang fra andre. Utstyr og ressurser skal holdes i forsvarlig stand og være tilgjengelig for KBO-enheten i ekstraordinære situasjoner.

4.4.1 Hensikten med bestemmelsen

KBO-enhetene skal ha rask og sikker tilgang på reservekomponenter der svikt kan medføre at forsyningen til kundene kan opphøre. Slik tilgang kan for eksempel sikres gjennom identifiserte reserveobjekter. Komponenter som det er vanskelig å skaffe eller som har lang leveringstid, må være tilgjengelig i et beredskapslager. De fleste enheter vil uansett ha på lager alminnelig materiell som også brukes i vedlikeholdssammenheng, eller de har avtale med en nærliggende grossist med lager.

Driften kan ofte opprettholdes ved omkoblinger eller ved midlertidige provisoriske tiltak. Eksempler på det siste kan være forberedt forbikobling av et bryterfelt i et koblingsanlegg. Andre ganger kan master i en luftledning være havarert eller en kabel gravd over. I slike tilfeller må det være tilgang på reservemateriell for provisorisk drift og utstyr for en permanent reparasjon.

Et viktig forhold er at det skal være sikker tilgang til materiell og utstyr i en ekstraordinær situasjon uavhengig av om ressursene eies av KBO-enheten eller av andre. Produksjonsrelaterte komponenter som turbiner, generatorer etc. forventes det ikke at KBO-enheten har på lager.

4.4.2 Reservemateriell

Enheten må ha tilgang til materiell og utstyr for gjenoppretting av nødvendige funksjoner etter skader og havari. Dette er av særlig stor betydning for kritisk viktig utstyr med lang leveringstid. Nødvendige ressurser kan være:

- Beredskapsmaster.
- Reservetransformatorer, transformatorolje og liknende.
- Store aggregater.
- Kabellengder og skjøter (sjø, luft, fjordspenn og liknende).
- Komponenter som effektbrytere, kompressorer, isolatorer og liknende.
- Transportutstyr og maskiner.
- Kraner og annet utstyr som er nødvendig for tunge løft.
- Fjernvarmerør, ventiler og pumper.
- Mobile varmesentraler.
- Datakomponenter og programvare for kritiske funksjoner.

Det er ikke et krav at enheten selv har alt dette, men enheten må vurdere behovet og sikre seg tilgang. Hvis enheten ikke selv har disse ressursene, må det inngås skriftlige avtaler med leverandører eller andre om hjelp. Enheten må sørge for at leverandører av kritisk viktige komponenter forplikter seg til å:

- Ha reservedeler i tilstrekkelig antall i en avtalt tid.
- Ha maksimale reparasjonstider for enkelte komponenter. Enheten bør avtale prioritet hos sine leverandører for å sikre rask respons under en ekstraordinær situasjon.
- Gi løpende informasjon om feil, mangler og andre svakheter på kritiske komponenter i anleggene, etter hvert som disse blir oppdaget.

4.4.3 Utstyr

Enheten må sikre seg nødvendig utstyr, herunder:

- Beredskapslager med kritisk viktig materiell og materiell med lang leveringstid.
- Avtale med leverandører med eget lager.
- Beredskapsmaster, reservetransformatorer, effektbryter, kabelskjøter, etc.
- Oppbevare beredskaps- og reservemateriell slik at ikke samme hendelse ødelegger både dette materiellet og de komponenter materiellet er reserve for.

Kravene til utstyr kan etterleves enten gjennom at KBO-enheten selv har tilstrekkelig med utstyr eller gjennom avtaler eller samarbeidsordninger, som eksempelvis *eBeredskap*.

Det vil være avgjørende med tilstrekkelig klare avtaler og at eventuelle samarbeidsordninger har et omfang og et innhold som gjør ordningen akseptabel.

4.4.3.1 Forsvarlig stand

Utstyr og ressurser som er nødvendig for sikrings- og beredskapstiltak, skal holdes i forsvarlig stand slik at det vil fungere etter forutsetningen i ekstraordinære situasjoner. Enheten bør derfor gjennomføre systematisk vedlikehold, modernisering eller erstatte gammelt utstyr med nytt, slik at dette utstyret og anleggene fungerer etter hensikten når behovet oppstår. Enheten bør legge spesiell vekt på dette for utstyr som sjelden er i bruk. Se også § 5-1 Sikringsplikt.

4.4.3.2 Tilgjengelighet

Enheten skal oppbevare materiell og utstyr slik at det er tilgjengelig for rask bruk uansett årstid, og med egnet transportberedskap. Det er et krav at disse ressursene er tilgjengelige i ekstraordinære situasjoner, også dersom de leveres av en underleverandør.

4.4.3.3 Oversikt og dokumentasjon

For at materiell og utstyr skal være tilgjengelig, er det behov for at enheten har oversikt over materiell og utstyr. Oversikten skal holdes oppdatert. Kravet gjelder ikke bare for reservemateriell og utstyr beregnet på energisystemer og anlegg, men også for driftskontrollsystemer med samband, relévern, driftsradio og andre nødvendige systemer. Ressursene kan deles inn i følgende grupper:

- Reserver for viktige komponenter/utstyr (som er i drift).
- Reparasjonsmateriell (for viktige deler av anlegg i drift).
- Strømaggregater.
- Tegninger, skjemaer og beskrivelser av viktige anlegg.
- Transportmateriell.
- Førstehjelps-/redningsmateriell.

Enheten må gjennomføre systematisk kontroll og vedlikehold av ovennevnte utstyr og øve på å bruke det.

4.4.4 Sikringstiltak og reservemateriell som det er gitt statstilskudd til etter tidligere forskrift

Gjennom årene er det gitt statstilskudd fra NVE til sikringstiltak og anskaffelse av reservemateriell etter søknad, med hjemmel i *forskrift om beredskap i kraftforsyningen*, § 7-2, eller etter andre tidligere bestemmelser. Vilårene som gjaldt da tilskuddet ble gitt, skal følges så lenge sikringstiltaket er relevant og reservemateriellet ikke har passert teknisk/økonomisk levetid.

Reserve- og beredskapsmateriell som det er gitt statstilskudd til, skal være fullverdiforsikret, oppbevares forsvarlig, vedlikeholdes og være tilgjengelig for andre KBO-enheter. Ved utløpet av utstyrets levetid skal NVE varsles. Enheten skal gi melding til NVE før slike sikringstiltak avvikles og før reservemateriell kondemneres. NVE avgjør i hvert enkelt tilfelle om avvikling eller kondemnering kan foretas.

Nytt og eksisterende beredskapsmateriell kan særbehandles gjennom inntektsrammereguleringen.

§ 4-5. Transport

Alle KBO-enheter skal ha en tilstrekkelig transportberedskap for å håndtere ekstraordinære situasjoner, og evne til rask gjenoppretting av funksjon. Dette omfatter tilgang til transportmidler med nødvendig utstyr og personer som kan håndtere disse.

For utstyr med transportvekt over 70 tonn, eller med store ytre dimensjoner, skal det utarbeides detaljerte transportplaner.

KBO-enhetenes transportmidler og private transportmidler tilhørende energiforsyningens personell som det er tjenstlig behov for, skal om mulig søkes fritatt for forberedt rekvirering til Forsvaret med videre.

4.5.1 Hensikten med bestemmelsen

Hensikten med denne bestemmelsen er å sikre tilgang til og sikker bruk av alle de transportmidler KBO-enheten måtte ha behov for i ekstraordinære situasjoner. Bestemmelsen gjelder alle typer kjøretøy fra lette personbiler via større kranbiler til tungt utstyr for spesialtransport, og inkluderer tilgang til helikopter og båt der det er nødvendig. For transport av det aller største og tyngste utstyret skal transportplanen også inkludere en vurdering av framkommelighet.

4.5.2 Planlegging av transportberedskapen

Transportberedskapen skal beskrives i KBO-enhetenes beredskapsplanverk eller som egne transportplaner for hvert anlegg. For å oppfylle kravet til transportberedskap, må KBO-enhetene enten eie transportmidlene selv, eller ha inngått skriftlige avtaler med andre som sikrer tilgang.

Det kan variere hvilke tungtransportmuligheter som er tilgjengelig i ulike deler av landet. KBO-enhetene skal ha en plan for transportberedskap og må ta stilling til om det må utarbeides spesialplaner som må avklares med Statens vegvesen, selv om utstyret ikke har transportvekt over 70 tonn. Dette vil bero på veistandard og aktuell transportvekt.

Planen for transportberedskap bør inneholde oversikt over:

- Kjøretøyer og transportutstyr som enheten eier.
- Eventuelt eksternt (eksempelvis lånt, innleid) utstyr av beredskapsmessig betydning.
- Spesialutstyr, for eksempel helikopter, terrenggående kjøretøy, mobilkraner med mer som kan bidra til å bedre den regionale beredskapen.
- Personell som har nødvendige sertifikater for å føre kjøretøyene.
- Verksteder som kan brukes til reparasjon i en ekstraordinær situasjon.
- Tilgang til drivstoff.
- Eventuelle andre forhold enheten finner relevant.

Det er svært viktig at planen for transportberedskap er gjennomførbar. Det vil blant annet si at planen må forberede beredskap for alternative transportruter ved uventede hendelser.

Der enheten er avhengig av eksterne ressurser, må dette kontraktfestes.

4.5.3 Transport av komponenter med transportvekt over 70 tonn eller store ytre dimensjoner

For å redusere konsekvensene ved havari av kritiske og tunge komponenter, som transformatorer, generatorer, turbiner, ventiler og rør, bør komponenten kunne repareres eller skiftes ut på kortest mulig tid. Både for reparasjon og utskifting er det nødvendig med en beredskapsplan for tungtransport. Enheten skal derfor ha transportplaner som gir oversikt over hvordan store og viktige komponenter kan transporteres. Oversikten bør angi:

- Type last.
- Vekt og største ytre dimensjoner.
- Opp- og avlastingssted.
- Opplastingsplass og transportrute med angivelse av spesielle forhold.
- Oversikt over hvilket utstyr som skal brukes.
- Kjøretillatelser.

Veier, jernbanenett og kaier kan være endret siden sist gang utstyret ble transportert, og kan gi uforutsette begrensninger. Det er derfor viktig at enheten avklarer dette på forhånd og holder transportplanene oppdatert.

4.5.4 Tilgang til drivstoff

I en krisesituasjon, for eksempel ved en rasjonering, vil bensinstasjonene kunne gå tomme for drivstoff før rasjonering settes i verk. Det er opp til hver enkelt enhet å skaffe seg nødvendig tilgang til drivstoff. Enheten bør vurdere å ha eget drivstoffanlegg, eller inngå avtale om prioritet hos leverandør av drivstoff. Rasjonering av drivstoff kan innføres ved erklært beredskap og i krig, etter *forskrift for oljerasjonering ved beredskap og krig*. Under knapphetssituasjoner i fredstid gjelder *forskrift om oljerasjonering ved oljeforsyningskriser i fredstid*.

4.5.5 Forberedt rekvirering av sivile kjøretøyer

Forsvaret, Sivilforsvaret og enkelte andre etater innen totalforsvaret kan ved krigsberedskap rekvirere sivile kjøretøyer. Kjøretøyer som tilhører KBO-enheter, og private kjøretøyer til nøkkelpersonell som av tjenstlige grunner har behov for egen transport, er fritatt for forberedt rekvirering. Fritaket er hjemlet i *Lov om militære rekvisisjoner* §§ 1 og 5. Forberedelse til rekvirering utføres etter Håndbok for forberedt rekvirering av sivile kjøretøyer (TH 100-12), Forsvarets Logistikkorganisasjon, 1984, ved kode 911 og 934.

- Ved registrering av nye kjøretøyer skal Statens vegvesen gjøres oppmerksom på at kjøretøyet skal være fritatt for forberedt rekvirering.
- Når kjøretøyer av denne kategorien leies eller leases, må enheten sørge for at også disse fritas fra forberedt rekvirering.

Dersom et kjøretøy likevel blir forhåndsrekvirert, bør enheten ta kontakt med rekvirerende myndighet, avklare eierforholdet, og vise til refererte hjemmel og koder.

Se nærmere om dette hos Statens vegvesen, omregistrering av kjøretøyer, [kodehefte autosys](#), kap 03, kjøretøyer som er fritatt fra militære rekvisisjoner, pkt. 14.

4.5.6 Sivil transportberedskap

Fylkeskommunen er den regionale myndigheten for sivil transportberedskap se *forskrift for sivil transportberedskap*. For at energiforsynings behov for kjøretøyer, drivstoff og reparasjonsberedskap i en ekstraordinær situasjon skal inngå i Fylkeskommunens plan, kan KBO-enhetens transportberedskapsplan samordnes med Fylkeskommunen.

§ 4-6. Nasjonal tungtransportberedskap

Statnett SF skal ha en nasjonal tungtransportberedskap for å sikre at tunge komponenter av betydning for energiforsyningen kan transporteres på kort varsel. Statnett SF skal vedlikeholde og oppgradere transportmidler med utstyr, samt anskaffe nye ressurser ved behov.

Statnett SF kan benytte den virksomhet som er etablert for å ivareta ansvar for tungtransportberedskap etter første ledd, til å utføre virksomhet for andre på markedsmessige vilkår. Endringer i virksomheten skal forelegges beredskapsmyndigheten for godkjenning.

Den nasjonale tungtransportberedskapen skal gjelde for ekstraordinære situasjoner, samt under beredskap og i krig.

Beredskapsmyndigheten kan treffe vedtak om organisering, bruk og finansiering av nasjonal tungtransportberedskap.

4.6.1 Hensikten med bestemmelsen

Statnett har et omfattende ansvar for tungtransportberedskapen i fred, ved beredskap og i krig. Tungtransportoppdrag for KBO skal utføres med materiell som skal befinne seg i landet når det er behov for det. Det er viktigere at det er kort mobiliseringstid enn at transportmidlene er i landet. Først under erklært beredskap og i krig, er det avgjørende at materiellet befinner seg i Norge. Tungtransport skal kunne utføres til alle havaristeder. Den type transport som er innbefattet, er angitt i § 4-5. Transport, annet ledd. Transportoppdrag utføres både som beredskapsoppdrag, og på vanlige forretningsmessige vilkår. Oppdragsgiver betaler i alle tilfeller for utførelsen av oppdraget.

Statnett SF disponerer gjennom sitt heleide datterselskap Statnett Transport AS transportmidler for tungtransport på jernbane, vei og til sjøs. Lufttransport må utføres med materiell som normalt ikke befinner seg i Norge. Endringer i virksomheten skal forelegges beredskapsmyndigheten for godkjenning.

4.6.2 Behov for tungtransportberedskap

Oppbyggingen av kraftforsyningssystemet med viktige knutepunkter som transformatorstasjoner og lange overføringslinjer, gjør at kraftforsyningen ikke fullt ut kan sikres mot ukontrollert strømutfall som følge av skader som skyldes naturgitte forhold, teknisk svikt eller tilsiktede ødeleggelser. Hovedtransformatorene – hvor kraften overføres fra hovednettet til fordelingsnettet – er de mest kritiske leddene. Havarier på disse enhetene kan forårsake omfattende utkoblinger og redusert kapasitet, med store samfunnsmessige konsekvenser som følge. For å redusere konsekvensene må de havarerte enhetene på kortest mulig tid kunne repareres eller skiftes ut med reserveenheter. Både for en eventuell reparasjon og utskifting, er det nødvendig med beredskap for transport av de tunge enhetene.

4.6,3 Statnett SFs rolle

Som eier av flertallet av landets tunge transformatorer og overføringslinjer og med en landsdekkende transportorganisasjon, skal Statnett SF innenfor Kraftforsyningens beredskapsorganisasjon (KBO) opprettholde en tungtransportberedskap, som på kort varsel skal kunne dekke energiforsyningens behov for transport av tunge enheter som transformatorer, generatorer og turbiner i fred, ved beredskap og i krig. Beredskapen skal bare omfatte transportoppdrag innen landets grenser, og skal gjennomføres ved bruk av materiell som befinner seg i landet.

4.6,4 Dekning av utgifter

Statnett SF skal administrere og organisere transportberedskapen og vedlikeholde maskinparken som transportberedskapen omfatter.

Utgifter knyttet til kapitalkostnader og opplæring av personell som skal betjene utstyret, blir dekket gjennom Statnett SFs nettariffer. Lagring og vedlikehold av utstyret og øvrige kostnader dekkes gjennom inntekter fra bruken av utstyret.

Statnett SF har ansvar for å foreslå nødvendige nyanskaffelser og oppgraderinger. I tvilstilfelle skal NVE avgjøre hvilke utgifter knyttet til transportberedskapen som skal henføres under beredskap eller forretning.

4.6,5 Klargjøringstid

I *fredstid* skal Statnett SF kunne iverksette transportoppdrag på kortest mulig tid, bare begrenset av transportmateriellets tilgjengelighet og klargjøring.

Ved *beredskap/krig* skal transportfunksjoner kunne iverksettes omgående når behov oppstår. Mannskaper som inngår i transportberedskapen skal være fritatt for annen tjeneste i Totalforsvaret.

4.6.6 Styring

I *fredstid* skal Statnett SFs transportorganisasjon styre bruken av transportmidlene på forretningsmessig grunnlag.

Ved *beredskap/krig* – etter at energiforsyningen er underlagt KBO – skal Kraftforsyningens sentrale ledelse (KSL) kunne disponere og koordinere bruken av transportmidlene.

§ 4-7. Samband

Alle KBO-enheter skal ha intern og ekstern sambandsberedskap for daglig drift, håndtering av ekstraordinære situasjoner og evne til rask gjenoppretting av nødvendige funksjoner for ledelse, drift og sikkerhet.

4.7.1 Hensikten med bestemmelsen

Kjernen i denne paragrafen er at samband er svært viktig i en ekstraordinær situasjon, særlig talesamband, og at det må etableres god beredskap for dette med ulike sambandsmidler. Samband skal til enhver tid være klart til bruk. Erfaring fra situasjoner med naturgitte hendelser viser at det må være god beredskap på dette området for å oppnå kontakt med lokale og regionale beredskapsmyndigheter, sårbare kunder og viktige samarbeidspartnere.

Nødnettet kan benyttes for å oppfylle kravet i denne paragrafen i de områdene av landet hvor det er utbygd og har tilfredsstillende dekning. Om ikke nødnettet eller eget mobilt radionett er tilgjengelig, må sambandsberedskapen ivaretas på annen måte, som for eksempel ved bruk av mobiltelefon, jaktradio eller annet.

4.7.2 Samband i ekstraordinære situasjoner

Pålitelige samband er av avgjørende betydning for sikker ledelse og drift, effektiv håndtering av ekstraordinære situasjoner og rask gjenoppretting av normal situasjon. Dette gjelder både innenfor den enkelte enheten i KBO, mellom ulike KBO-enheter i et område og til andre relevante aktører.

Enheten skal alltid ha mulighet til å kommunisere med personell som er viktig for å opprettholde energiforsyningen, også under ekstraordinære situasjoner.

- Nødvendig personell som må tilkalles.
- Montører og annet personell ute i felten.
- Personell i stasjoner.
- Personell ved andre kontorer i samme KBO-enhet.
- Andre KBO-enheter man har behov for å kommunisere med.
- Viktige eksterne leverandører, for eksempel entreprenører og leverandører av driftskontrollsystem.
- Myndigheter.

Samme krav gjelder for samband til utstyr eller komponenter for styring av nettet. Ved svikt bør det finnes alternativer som raskt kan etableres. For nærmere krav til driftskontrollsystemer og mobile radionett - driftsradio, se kapittel 7.

KBO-enheten må for sine egne sambandssystemer sørge for at:

- Enheten har nødvendig reparasjonsmateriell for sitt sambandssystem.
- Det er tilstrekkelig nødstrøm til sambandssystemene.

Enheten må være oppmerksom på at mobilnettet kan slutte å virke etter relativt kort tid ved roterende utkobling eller overlast i nettet. Det samme gjelder IP-basert telefonnett.

4.7.3 Dokumentasjon, beredskapsforhold og daglig drift

Enheten bør bruke alle typer samband som er beskrevet i beredskapsplanen i daglig drift for å sikre at personellet som skal bruke sambandet, har tilfredsstillende kompetanse til å håndtere det raskt og sikkert. Enheten må øve på bruken jevnlig.

Dokumentasjon bør omfatte:

- Oversikt over sambandsmidler enheten har behov for.
- Plan og rutiner for opplæring av nødvendig sambandspersonell.
- Oversikt over leide samband og deres funksjonalitet under strømbrudd.
- Sambandsutstyrets viktigste egenskaper og funksjoner under ekstraordinære forhold.
- Vedlikeholdsrutiner og logg over vedlikehold for eget utstyr.
- Avtaler med eksterne leverandører for vedlikehold, reparasjoner etc. (se også punkt under om eksterne leverandører).
- Rutiner og hyppighet for test av reserveløsninger og logging av dette.

Det er viktig at enheten inkluderer sambandsberedskap i beredskapsplanverket for å være i stand til rask og effektiv håndtering av ekstraordinære situasjoner. I planen må det minst inngå:

- Oversikt over de sambandsmidler enheten disponerer, og hvor utstyret befinner seg.
- Oversikt over personell som kan bruke/ reparere sambandet. Dette inkluderer blant annet personell i driftssentralen, ledelsen, reparasjonspersonell, personell som skal styre klassifiserte anlegg lokalt. Disse må ha nødvendig kompetanse.
- Oversikt over reserveløsninger.
- Alternative sambandsmuligheter.

4.7.4 Eksterne leverandører av sambandstjenester – avtaler

Ved kjøp av teletjenester til kritiske samband bør vesentlige forhold som dreier seg om leveransesikkerheten for tjenesten kontraktfestes. Noen av de forholdene som må avklares, er:

- Nødstrøm og reserveforsyning til relevante sentraler og kommunikasjonsnett.
- Redundans, tilgjengelighet (kapasitet, oppetider).
- Prioritet som kan gis ved trafikksperr og feilretting.
- Evne til håndtering av større feil i kritiske situasjoner.

Man bør også forsikre seg om at leverandøren virkelig er i stand til å holde hva vedkommende lover i en kritisk situasjon. For eksempel kan leverandøren ha tilsvarende avtaler med andre aktører i tilknyttet område, som samtidig har behov for assistanse ved store og omfattende utfall.

Ved kjøp av ekom-tjenester kan det være hensiktsmessig å inngå avtale om tjenestekvalitet: Service leveringsavtale (SLA). En slik avtale kan også være nyttig som sjekkliste ved mindre omfattende avtaler.

For krav til mobile radionett - driftsradio, se § 7-17.

Kapittel 5. Klassifisering og sikringstiltak

Klassifisering

Energiforsyningsanlegg blir nå som hovedregel klassifisert på bakgrunn av de ytelses- og spenningskriteriene som er angitt i § 5-2 i forskriften. Dermed vil sikringsklasse være kjent når det søkes om konsesjon for nye anlegg. Konsesjonssøkere/ konsesjonærer kan og skal planlegge og innarbeide relevante sikringstiltak på et tidlig tidspunkt i planleggingsprosessen.

Det kan fattes enkeltvedtak etter § 5-7 dersom det skulle vise seg at et anlegg har eller får en vesentlig større eller mindre betydning enn det som kriteriene i § 5-2 skulle tilsi. Dersom konsesjonssøker mener at et anleggs faktiske betydning ikke samsvarer med den klassen som følger av forskriften, kan det sendes en begrunnet søknad til NVE om endring av klasse. På den måten kan et eventuelt enkeltvedtak foreligge samtidig med at NVE gir konsesjon.

Tilsvarende kan også beredskapsmyndigheten på eget initiativ vedta en annen klasse enn det som framgår av forskriften.

Sikringstiltak

Kravene til sikringstiltak videreføres og innebærer lite nytt for de virksomhetene som til nå har fulgt regelverket.

Som følge av ny § 9-2 i *energiloven* er sikringsplikten tydeliggjort for alle som eier eller driver energianlegg mv., og omfatter nå både anlegg og ressurser etter kapittel 4 om ressurser og reparasjonsberedskap.

En rekke viktige punkter som tidligere var veiledning er nå blitt forskrift i form av vedlegg 1-3 til bfe under sikring av de enkelte klasser §§ 5-4, 5-5 og 5-6.

Kapittel 5 må også leses i sammenheng med overgangsbestemmelsene i § 8-9, hvor det framgår at fysisk sikring av eldre anlegg kan tilpasses bygningsteknisk utforming og tidligere pålegg om fysisk sikring.

NVE påpeker at forskriftens krav til sikringstiltak også gjelder for eksisterende anlegg. For øvrig vises det til overgangsbestemmelsen - § 8-9.

§ 5-1. Sikringsplikt

Eier eller driver plikter å sikre anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende. Med anlegg menes her også bygg og andre ressurser omfattet av kapittel 4.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter anleggets eller systemets type, oppbygging og funksjon.

Alle anlegg m.m. som nevnt i første ledd skal holdes i funksjonsdyktig stand og skal så langt som mulig virke etter sin hensikt under ekstraordinære forhold.

Det skal særlig tas hensyn til ekstraordinære forhold som:

- *uvær og annen naturgitt skade*
- *brann og eksplosjoner*
- *alvorlig teknisk svikt*
- *innbrudd, hæververk, sabotasje og andre kriminelle handlinger*

5.1.1 Hensikten med bestemmelsen

Hensikten med denne bestemmelsen er å sørge for at det er etablert et minimum av sikringsnivå mot uønskede hendelser og handlinger ved alle anlegg, bygg, systemer, ressurser og annet av betydning for energiforsyningen

Bestemmelsen pålegger alle som eier og driver energiforsyningsanlegg mv. en selvstendig plikt til å vurdere og iverksette sikringstiltak ved de anleggene selskapet har ansvar for.

Det skal tas hensyn til at ressurser mv. etter denne forskrifts kapittel 4 skal sikres så langt dette omfatter beredskapstiltak, jf *energiloven* § 9-2, 3 ledd.

5.1.2 Hvem sikringsplikten gjelder for

Sikringsplikten gjelder for alle som helt eller delvis eier eller driver anlegg eller system, eller som har ressurser som nevnt ovenfor.

For konsesjonspliktige anlegg vil dette primært gjelde den som har fått konsesjon, men også driftsansvarlige og eiere uten konsesjon av relevante bygg, eiendom, grunn og andre ressurser plikter å sikre anlegg og øvrig virksomhet etter denne bestemmelsen.

For anlegg som ikke er konsesjonspliktige, som for eksempel driftskontroll- og sambandsanlegg, og ressurser som for eksempel lagerbygg og reservemateriell, omfatter bestemmelsen plikt til å oppfylle kravene til beredskapstiltak. Plikten gjelder både eier og driver slik disse fordeler ansvar og råderett seg i mellom.

Første ledd omfatter også en bestemmelse om adgang for uvedkommende – se eget punkt om adgangskontroll under.

5.1.3 Virksomhetens plikter

Andre ledd innebærer at virksomhetene skal planlegge, gjennomføre og vedlikeholde sikringstiltak etter anleggets eller systemets type, oppbygging og funksjon. For KBO-enheter vil dette være en konsekvens av risiko- og sårbarhetsanalyser (jf § 2-4 Risiko- og sårbarhetsanalyse og jf § 5-8 Analyse for klassifiserte anlegg), som tar hensyn til stedlige forhold og risiko. Se også § 2-10 Internkontrollsystem og eget punkt under om kontroll og vedlikehold.

Det bør også være en riktig balanse i sikringstiltakene, for klassifisert anlegg er dette et krav (se sikring av klassifiserte anlegg, § 5-4 til § 5-6 om sikringstiltak for klasse 1 til 3 med vedlegg 1 til 3 om særlige krav til sikring av anlegg også. Det er for eksempel

begrenset virkning av en solid dør dersom usikrede vinduer på bakkeplan gir adkomst til de samme arealene.

5.1.4 Anleggene skal holdes i stand og virke etter hensikten

Tredje ledd inneholder et generelt krav om at alle anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner (jf første ledd), skal holdes i funksjonsdyktig stand og så langt som mulig virke etter sin hensikt under ekstraordinære forhold.

Dette kravet er viktig for å kunne håndtere en ekstraordinær situasjon. Kravet framgår også av konsesjonsvilkårene for konsesjonspliktige anlegg, jf *energilovforskriften* § 3-5 c. Tredje ledd understreker at krav til beredskap ikke bare gjelder forberedte og ytre sikringstiltak, men også krav til at anleggene fungerer som de skal i en ekstraordinær situasjon når behovet er størst.

For et anlegg som blir rammet av en uønsket hendelse eller handling, skal sikrings-tiltakene være innrettet slik at anlegget likevel så langt som mulig skal virke etter sin hensikt. Vi vil her peke på at forbyggende tiltak, redundans i anlegg og system og evne til å håndtere og gjenopprette anleggets funksjon er viktige deler av beredskapen. Sikringsplikten må ses i sammenheng med disse elementene i regelverket.

5.1.5 Virksomhetene skal ta hensyn til ekstraordinære forhold

Henvi­sing til begrepet ”kriminelle handlinger” i fjerde ledd omfatter handlinger som er straffbare etter *straffeloven* og andre straffebestemmelser i lovgivningen, samt forhold som ikke er dekket av noen straffebestemmelse, men anses klart samfunnsmessig uakseptable. Opp­lis­tingen av kriminelle handlinger er ikke uttømmende. Kriminelle handlinger omfatter også terror. Sabotasje omfatter alle former for bevisst skadeverk og ødeleggelse, både fysisk og elektronisk.

Fjerde ledd er heller ikke uttømmende. Tiltakene skal også ta hensyn til overlagte uønskede handlinger og forberedelser til slike. I den sammenheng kan egne nåværende og tidligere ansatte utgjøre en risiko for virksomheten i form av utroskap eller trusler. Bestemmelsen er utformet slik at den skal dekke overlagte uønskede handlinger slik det framgår av § 3 i *lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)*.

5.1.6 Nærmere om adgangskontroll

Første ledd inneholder en bestemmelse om å sikre anlegg, system, ressurser (jf kapittel 4 Ressurser og reparasjonsberedskap) med videre mot adgang for uvedkommende. Det er her også relevante bestemmelser i § 5-3 Sikring av klassifiserte anlegg, § 5-4 til § 5-6 om sikringstiltak for klasse 1 til 3 med vedlegg 1 til 3 (til bfe) om særlige krav til sikring av anlegg, § 5-11 Besøksrestriksjoner og § 7-1 Generell plikt til å beskytte driftskontrollsystemet.

Etter disse bestemmelser skal adgangskontroll blant annet omfatte følgende:

- Driftssentraler, sambandsanlegg og rom med tilhørende utrustning for driftskontroll og lokalkontroll i klassifiserte anlegg.
- Bygg og områder med klassifiserte energiforsyningsanlegg.

- Bygg for ledelse, drift og andre vesentlige ressurser for beredskap, drift, sikkerhet og gjenoppretting.
- Lagerområder ute og inne for materiell, kjøretøy og annet av vesentlig betydning for beredskap, drift, sikkerhet og gjenoppretting.
- Beredskapsrom og rom med IKT-utstyr av betydning for beredskap, drift og sikkerhet.

Det skal etableres adgangskontroll både for fysiske og elektronisk avgrensede områder (jf også § 6-3 Beskyttelse, avskjerming og tilgangskontroll og § 7-4 Kontroll med brukertilgang). Med adgangskontroll menes en kontroll med hvem som ut fra en tjenstlig vurdering skal ha selvstendig adgang til ett eller flere av de ovennevnte områdene. Det omfatter også hvem som kan gis adgang i følge med eller under oppsyn av en person som har selvstendig adgang. For alle andre skal området være effektivt avstengt.

Virksomheten kan etablere adgangskontroll med kombinasjoner av avlåsning, vakthold, overvåking, registrering og/eller ved bruk av andre tekniske løsninger. Disse må være av en tilstrekkelig høy kvalitet. Det må være et logisk samsvar mellom adgangskontroll og fysiske sikringstiltak.

Virksomheten må innarbeide en rutine for å kontrollere at porter, dører og vinduer fungerer etter hensikten og lar seg lukke og låse. Virksomheten må ha full kontroll med tilgangsrettigheter for nøkkelkortsystemer. Der nøkkelkort brukes, må det kombineres med bruk av pin-kode for atkomst/tilgang. Alminnelige låsesystemer er sårbare for at nøkler mistes, og virksomheten må ha rutiner for administrering, slik at nøkler på avveie oppdages og at relevante tiltak blir gjennomført. Det bør brukes adgangskontrollsystemer som kan logge aktivitet. Slike logger bør gjennomgås jevnlig for å avdekke hendelser av sikkerhetsmessig betydning.

5.1.6.1 Adgangskontroll ved driftssentraler mv.

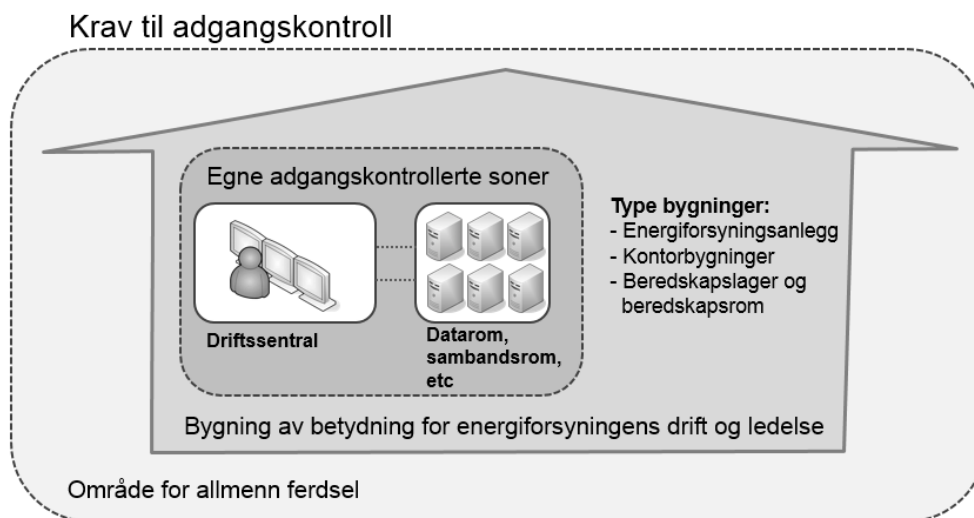
Driftssentraler med tilhørende utrustning omfatter (jf Sikring av klassifiserte anlegg, § 5-4 til § 5-6 om sikringstiltak for klasse 1 til 3 med vedlegg 1 til 3 til bfe om særlige krav til sikring av anlegg og kapittel 7 Beskyttelse av driftskontrollsystem):

- Driftssentraler, sambandsanlegg og øvrige anlegg og rom med komponenter som ivaretar driftskontrollfunksjoner eller kan gi fysisk eller elektronisk adgang til slike.
- Alle deler av bygningen eller anlegget der driftssentralen, operatørrom, prosessanlegg, viktige IT- og sambandsanlegg og nødstrøm er plassert.
- Alle rom der driftskontroll kan utøves, som f.eks. styring av koblinger og overvåking av tilstand i anleggene.

Slike steder skal være egne adgangskontrollerte sikkerhetssoner. Virksomheten må holde disse rommene avlåst for alle som ikke har selvstendig adgang. Personer kan få selvstendig adgang gjennom autorisering. Øvrige skal ledsages av personer som har gyldig autorisasjon. Dersom virksomheten har bærbar utstyr som kan brukes til styring og kontroll av kraftsystemkomponenter utenfor driftssentralen, for eksempel på eget kontor eller hjemmevakt, se § 7-10 Ekstern tilkobling til driftskontrollsystem. Se for øvrig også § 7-4 Kontroll med brukertilgang.

Sikkerhetssonen skal være utstyrt med adgangskontrollsystemer av en slik kvalitet at et innbrudd eller innbruddsforsøk vil etterlate synlige spor. For ytterligere krav til sikring av driftskontrollsystemer, se veiledning til kapittel 7 Beskyttelse av driftskontrollsystem. For veiledning om fysiske barrierer, se veiledningen til bestemmelsene om sikringsnivå under § 5-4, 5-5 og 5-6.

Figur 5-1 Figuren under viser prinsipp for adgangskontroll til driftssentral, 2 nivå, ytre og indre sone.



5.1.6.1 Adgangskontroll ved bygge- og installasjonsarbeid

I anleggsfasen må virksomheten etablere adgangskontroll senest fra det tidspunkt installasjonsarbeidene begynner. Alle faste adgangsberechtigede skal utstyres med adgangskort. Tilfeldige arbeidstakere, leverandører, besøkende og liknende skal gis tidsbegrensede adgangskort. Kjøretøyer skal være registrert og ha parkeringstillatelse. For besøkende, se også § 5-11 Besøksrestriksjoner.

5.1.7 Nærmere om kontroll og vedlikehold

Med sikringstiltak jf andre ledd forstås her tiltak ifølge bestemmelsene i denne forskriften.

Andre ledd inneholder en bestemmelse om at den enkelte virksomhet blant annet har ansvar for vedlikehold av sikringstiltak. Her viser vi også til § 2-10 Internkontrollsystem og § 5-3 Sikring av klassifiserte anlegg.

For at virksomheten skal kunne føre tilstrekkelig kontroll og vedlikehold med sikringstiltakene på anlegget, må virksomheten ha oversikt over hvilke sikringstiltak som er pålagt og gjennomført. Dette gjelder både de sikringstiltakene som er i daglig bruk, og de som er passive.

Virksomheten må sørge for at følgende blir gjennomført og dokumentert:

- Identifisere hvilke sikringstiltak som er pålagt og gjennomført for anlegget.
- Føre en oppdatert oversikt over sikringstiltakene, både aktive og passive.
- Ha en oppdatert beredskapsplan for bruken av tiltakene, når tiltakene skal settes i verk, hvem som skal gjøre hva og hvilke ressurser det er behov for (verktøy, maskiner, med mer).

- Innarbeide kontroll og vedlikehold av sikringstiltakene i virksomhetens vedlikeholdssystem/kvalitetssystem, som sikrer en fornuftig frekvens på kontrollene.
- Funksjonsteste sikringstiltakene jevnlig for å se om de fungerer etter hensikten. Dette er spesielt viktig for de passive sikringstiltakene.
- Sørge for at defekte tiltak erstattes eller repareres.
- Andre nødvendige tiltak for at sikringstiltakene fungerer hensiktsmessig.

Materiell og utstyr til sikringstiltak som ikke er i daglig bruk, må oppbevares hensiktsmessig, slik at det ikke blir ødelagt. I tillegg må sikringstiltakene være tilgjengelige og håndterbare, slik at de raskt kan settes i verk ved behov.

5.1.8 Forholdet til annet regelverk

NVE legger til grunn at alle lover og forskrifter som ut fra energilovens hensyn stiller relevante krav til sikringstiltak og øvrig bygningsmessig utførelse, følges. Dette gjelder relevante krav etter *plan- og bygningsloven* og særlig krav til brannsikring, hvor en del energiforsyningsanlegg med hjemmel i *brann- og eksplosjonsvernloven* er identifisert av vedkommende kommune som særskilte brannobjekter. I det etterfølgende gir vi henvisninger til en del av det regelverket som er av betydning for det totale sikringsnivået. Denne oversikten er ikke uttømmende.

Beredskapsforskriften med veiledning setter i noen tilfeller strengere krav til sikringstiltak enn lover og forskrifter som er omtalt nedenfor. Men det kan også forekomme at angitte tiltak som er veiledende minimum for å beskytte energianlegget mot uønskede hendelser og handlinger, ikke alltid tar hensyn til konstruksjonsmessige og liknede krav. Det forutsettes derfor at bygnings-, brann- og elektrotekniske krav til både bygninger, øvrige konstruksjoner og elektriske komponenter beregnes og utføres etter gjeldende regler og normer. Dette kan resultere i økte, men ikke reduserte, krav til konstruksjon og utførelse.

- *Lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver* (brann- og eksplosjonsvernloven) av 14. juni 2002, med forskrifter.
- *Forskrift om brannforebyggende tiltak og tilsyn* (forebyggendeforskriften), fastsatt av Direktoratet for samfunnssikkerhet og beredskap (DSB) 26. juni 2002.
- *Temaveiledning – brannvern i kraftforsyningen*, Direktoratet for samfunnssikkerhet og beredskap (DSB) og Norges vassdrags- og energidirektorat (NVE), november 2003.
- *Lov om planlegging og byggesaksbehandling* (plan- og bygningsloven - pbl.) av 27. juni 2008, med forskrifter.
- *Forskrift om tekniske krav til byggverk* (Byggteknisk forskrift – TEK 10) av Kommunal- og regionaldepartementet, 26. mars 2010

- *Forskrift om elektriske forsyningsanlegg (FEF)* fastsatt av DSB 20. desember 2005, i kraft 1. januar 2006 med hjemmel i lov 24. mai 1929 nr. 4 om tilsyn med elektriske anlegg og elektrisk utstyr. Veiledning til *FEF* fastsatt av DSB i 2006.
- *Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg (FSE)*, fastsatt av 28. april 2006 med hjemmel i lov 24. mai 1929 nr. 4 om tilsyn med elektriske anlegg og elektrisk utstyr.
- *Forskrift om objektsikkerhet*, fastsatt ved kgl.res. 22. oktober 2010 med hjemmel i lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven). Det gjøres samtidig oppmerksom på at bestemmelser etter denne ikke er gjort gjeldende for energiforsyningen, men ivaretas av beredskapsforskriften.
- *Forskrift om behandling av personopplysninger* (personopplysningsforskriften), Fastsett ved kgl.res. 15. desember 2000 med hjemmel i lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
- *Lov om petroleumsvirksomhet* (petroleumsloven) av 29. november 1996 med forskrifter, er relevant for bl.a. gassdrevne kraftverk.
- For krav til innbrudds- og hærverkssikring kan virksomheten ta utgangspunkt i kravene om Forsikringsselskapenes Godkjennelsesnemnd (FG) setter til relevante dører, porter, vinduer og lignende med innfesting, karmen og låseanordninger. Her vises det også til gjeldende Europeiske normer, se veiledning om sikringstiltak under §§ 5-4, 5-5 og 5-6.
- Norsk Elektroteknisk Komite (NEK) bl.a. NEK 400:2010 *Elektriske lavspenningsinstallasjoner* og NEK 445:2009 *Luftledninger over 1 kV* bør følges dersom ikke denne forskrift stiller andre eller strengere krav.
- Norsk Elektroteknisk Komite (NEK), NEK 440:2011 *Stasjonsanlegg over 1 kV*.
- Norsk Elektroteknisk Komite (NEK), 445:2009 *Luftledninger over 1 kV*.

Virksomheten er selv ansvarlig for å holde seg orientert om eventuelle endringer i overnevnte regleverk og standarder.

§ 5-2. Klasser

Ved klassifisering av anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme benyttes klasse 1 til 3. Klasse 3 benyttes der betydningen for energiforsyningen er størst.

Koblingsanlegg, kraftledning, mufteanlegg, lokalkontrollanlegg og annet som funksjonelt er en del av en kraft-, transformator- eller omformerstasjon klassifiseres etter vedkommende stasjons klasse.

Denne bestemmelse omfatter ikke energianlegg for rene industriformål eller energianlegg som eies av en virksomhet som selv er eneste sluttbruker av energien fra anlegget.

Denne bestemmelse omfatter ikke midlertidige energianlegg eller midlertidige løsninger som del av energianlegg når det foreligger konkrete planer for utbygging eller oppgradering av spenningsnivå.

I ytelseskriteriene i denne bestemmelse medregnes ikke mobile komponenter som reserveaggregat eller beredskapstransformatorer, midlertidige plasserte transformatorer, generatortransformatorer, eller transformatorer for regulering og spesielle formål (fasekompensering, spoler og lignende). For transformatorer med flere funksjoner (viklinger) regnes høyeste ytelse av transformering mellom nettnivåer.

Klasse 1 omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 25 MVA.*
- b. Transformatorstasjon med samlet hovedtransformatorytelse på minst 10 MVA.*
- c. Omformerstasjon med samlet installert ytelse for omforming på minst 10 MVA.*
- d. Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 30 kV.*
- e. Kraftledning bygget for et spenningsnivå på minst 5 kV.*
- f. Fjernvarmesentral med samlet installert ytelse på minst 50 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.*
- g. Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til d og f.*

Klasse 2 omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 100 MVA og kraftstasjoner på minst 100 MVA plassert i dagen.*
- b. Transformatorstasjon med samlet hovedtransformatorytelse på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.*
- c. Omformerstasjon med samlet installert ytelse for omforming på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.*
- d. Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 100 kV.*
- e. Kraftledning bygget for et spenningsnivå på minst 30 kV.*
- f. Fjernvarmesentral med samlet installert ytelse på minst 150 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.*
- g. Driftskontrollsystem plassert i klasse 2 etter enkeltvedtak.*

Klasse 3 omfatter:

- a. Kraftstasjon i fjell med samlet installert generatorytelse på minst 250 MVA.*

- b. *Transformatorstasjon med samlet hovedtransformatorytelse på mer enn 100 MVA og bygget for et høyeste spenningsnivå på minst 200 kV og transformering til sekundært spenningsnivå i nett på minst 30 kV.*
- c. *Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 200 kV.*
- d. *Kraftledning bygget for et spenningsnivå på minst 200 kV.*
- e. *Driftskontrollsystem plassert i klasse 3 etter enkeltvedtak.*

5.2.1 Hensikten med bestemmelsen

Hensikten med denne paragrafen er å etablere et enkelt, logisk og forutsigbart system for å differensiere krav til sikringsnivå i tre klasser etter hvilken betydning de ulike anleggene har for energiforsyningen. Som operasjonelle kriterier angis ytelse og nettnivå ved spenning.

5.2.2 Klassifiseringssystemet – endringer og overgangsregler

Alle klassifiserte kraftforsyningsanlegg ble gjennomgått og fikk enten beholde eller gitt ny klasse ved NVEs vedtak *Kraftforsyningsanlegg – besøksrestriksjoner – klassifisering* av 23. februar 1996. Fra da og til og med 2002 fattet NVE enkeltvedtak om klassifisering etter kriterier, klasseinndeling og krav til sikringstiltak etter den tidligere "Retningslinjer for sikring av kraftforsyningsanlegg" (siste utgave: NVE november 1997), i tre klasser hvor klasse 1 var strengest.

Fra 2003 og fram til og med 2012 har NVE fattet enkeltvedtak om klassifisering av anlegg og sikringstiltak, etter kravene i den tidligere beredskapsforskriften (BfK). Her ble klasseinndelingen snudd slik at klasse 3 ble den strengeste. Dette ble i 2003 automatisk gjort gjeldende for alle klassifiserte anlegg uten at det ble fattet nye enkeltvedtak.

I dag finnes det rundt 1 500 klassifiserte anlegg. Av disse er rundt en tiendedel klassifisert fra og med 2003 (etter BfK). Pr. 2012 var fremdeles det store flertallet anlegg klassifisert etter vedtaket fra 1996, ut fra datidens kraftsystem og regelverk, kriterier og praksis. Mange anlegg er blitt ombygd og utvidet siden den gang, uten at det er sendt melding til NVE, og dermed uten at det er vedtatt ny tilpasset klasse.

Denne paragrafen om forskriftsmessig klassifisering vil etter overgangsbestemmelsene i § 8-9 virke på følgende måte:

Alle anlegg klassifisert ved enkeltvedtak etter BfK i perioden f.o.m. 2003 t.o.m. 2012 beholder sin klasse inntil annet eventuelt blir vedtatt.

Alle anlegg klassifisert før 2003 får automatisk klasse etter denne bestemmelsen. Unntatt er driftssentraler i klasse 2 og 3 som beholder sin klasse uansett når de er klassifisert inntil annet eventuelt blir vedtatt.

Nye og andre anlegg som oppfyller kriteriene i bestemmelsen, og som ikke tidligere er meldt til NVE og klassifisert, får automatisk klasse etter denne bestemmelsen.

5.2.3 Nærmere om hensikten

Klassifisering etter disse bestemmelsene er fastsatt ut fra et overordnet nettstrategisk perspektiv hvor det blant annet tas hensyn til hvor omfattende et utfall kan bli, og hvor lang tid det tar å reparere anlegget og dermed gjenopprette forsyning ved omfattende skader.

Operasjonelt er bestemmelsene i § 5-2 fastsatt ut fra et enkelt og logisk system for klassifisering etter anleggenes ytelse og nettnivå, hvor sentralnettanlegg i hovedsak plasseres i klasse 3, regionalnettanlegg i klasse 2 og lokale fordelingsnett i klasse 1. Det er valgt en lignende logikk for fjernvarmeanlegg.

Slike generelle bestemmelser kan vanskelig være helt treffsikre for alle anlegg i hele landet. Slik kan for eksempel sentralnettet (132 kV) enkelte steder være svakere dimensjonert enn deler av 132 kV regionalnettet i andre områder. Tilsvarende vil en middels kraftstasjon kunne anses som en stor og viktig stasjon for et viktig lokalt forsyningsområde som ikke har egen kraftproduksjon.

Dersom disse bestemmelser ut fra en beredskapsmessig vurdering av forsynings-sikkerheten gir feilaktig eller urimelige utslag for et anlegg, kan NVE etter en særskilt vurdering foreta endringer ved enkeltvedtak etter § 5-7. Her kan særlig viktige anlegg for lokal forsyning vurderes særskilt og gis en høyere klasse. Det kan også gis unntak for mindre viktige anlegg slik at disse, etter initiativ fra NVE eller på grunnlag av en begrunnet søknad, gis en lavere klasse.

5.2.4 Virkning av forskriften

Forskriften medfører en reduksjon i antall høyt klassifiserte kraftstasjoner. Dette gjenspeiler en forskyvning av beredskapsmessig vektlegging fra produksjon til nett og driftskontrollsystemer, og en vektlegging av å sikre de viktigste anleggene. Som følge av utbygging av sentralnettet, kan det over tid bli en økning i antall transformatorstasjoner i klasse 3.

Et anleggs klasse er kjent når det søkes om konsesjon for nye anlegg. Konsesjonssøker/konsesjonærer skal derfor planlegge og innarbeide relevante sikringstiltak for anlegget som en del av planleggingsprosessen.

5.2.5 Anlegg som inngår i klassifiseringen

”Dammer og vassdragsreguleringsanlegg” omfattes ikke av klassifisering etter denne bestemmelsen. Slike anlegg klassifiseres etter *forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften)*. Bestemmelsen i § 5-7 gir (jf. *energiloven* § 9-2) likevel hjemmel til å treffe enkeltvedtak om sikringstiltak også for dammer og vassdragsreguleringsanlegg av vesentlig betydning for kraftproduksjon som tillegg til den generelle sikringsplikten. Men normalt vil damsikkerhetsforskriftens krav også oppfylle denne forskriftens krav til fysisk sikring av relevante anlegg.

”Fjernvarmesentraler” – det anlegget som skal sikres, omfatter hele varmesentralen med alle bygninger som inneholder kjeler med nødvendige installasjoner.

”Kraftstasjoner”, ”transformatoranlegg” mv. omfatter hele anlegget med alle elektrotekniske, mekaniske og bygningsmessige installasjoner, tilhørende anleggsdeler og

annen utrustning. For vannkraftstasjoner vil dette også omfatte den del av vannveien som har direkte betydning for drift og sikring av stasjonen.

”Omformerstasjon” omfatter i praksis like-/vekselretting for store likestrømsoverføringsanlegg. Bestemmelsen omfatter i praksis ikke lenger omforming for jernbane og sporveisdrift, men her gir likevel bestemmelsen i § 5-7 (jf *energiloven* § 9-2) hjemmel til å treffe enkeltvedtak om sikringstiltak.

”Kraftledning” omfatter enhver ledning som kan overføre elektrisk kraft (vekselstrøm eller likestrøm), både luftledning og kabel (sjø og land) med tilhørende elektriske og bygningstekniske installasjoner, herunder muffeanlegg, brytere og lignende når dette ikke er del av et annet anlegg. Den omfatter også den fysiske ledningstraseen så langt denne har beredskapsmessig betydning for sikring, drift og gjenoppbygging.

For ”driftskontrollsystemer” vil det som nå foretas individuell saksbehandling, men driftskontrollsystemer som til nå ikke er klassifisert, havner automatisk i klasse 1. For å bli klassifisert forutsettes det likevel at det er et IKT- basert prosesskontrollsystem (mini Supervisory Control And Data Acquisition - SCADA e.l.) av betydning for overvåkning eller drift av anlegg etter denne paragrafen. Driftskontrollsystemer plasseres i klasse 2 eller 3 etter enkeltvedtak, jf meldeplikt etter § 5-9 . Eksempelvis er det ikke nødvendigvis slik at en virksomhet som har ett til to kraftforsyningsanlegg i klasse 3 også får driftskontrollsystemet sitt klassifisert i klasse 3. Derimot kan en virksomhet som for eksempel har mange kraftforsyningsanlegg i klasse 2 som styres fra driftskontrollsystemet, få dette plassert i klasse 3.

5.2.6 Anlegg med flere funksjoner og eiere

En del kraftforsyningsanlegg ivaretar ulike funksjoner (produksjon, sentralnett, regionalnett med mer) i kraftsystemet, og ulike anleggsdeler kan være fordelt på flere eiere. Hvor dette er naturlig, og der det er sammenfall mellom fysisk og elektrisk inndeling, funksjon og eier, kan anlegget deles opp slik at de ulike deler får ulik klasse. Andre steder vil forholdene tilsi at anlegget som helhet gis en klasse etter viktigste funksjon(er) eller summen av ulike funksjoner.

Dersom et anlegg - som det ikke er naturlig å dele opp i flere ulikt klassifiserte anlegg - har flere funksjoner, **vil det være den viktigste funksjonen som angir anleggets klasse.** Det vil i praksis si at det er det punktet i denne bestemmelsen som gir høyeste klasse som vil være bestemmende for anleggets klasse. Sekundære deler av anlegget kan likevel etter en analyse i det enkelte tilfellet jf § 5-8, sikres etter lavere klasse bestemt for denne anleggsdelen.

Eksempel:

Dersom det i en 420 kV selvstendig koblingsstasjon i klasse 3 settes inn en 40 MVA transformator for lokal forsyning, blir ikke dette dermed en transformatorstasjon i klasse 1. Eventuelt kan anlegget da betraktes som en koblingsstasjon i klasse 3 og en transformatorstasjon i klasse 1. Det forutsettes at sist nevnte funksjonelt og fysisk kan skilles fra øvrige anlegg.

5.2.7 Klassifisering i tre klasser

Som tidligere klassifiseres anlegg i tre klasser der klasse 3 er den strengeste klassen ut fra den betydningen den har for forsyningssikkerheten og for å kunne håndtere ekstraordinære situasjoner. Før øvrig viser vi til de innledende punktene i dette kapitlet.

5.2.8 Klassifisering av ulike typer anlegg

Koblingsanlegg og muffeanlegg som funksjonelt tilhører en kraft- eller transformatorstasjon, blir regnet som en del av denne, og får klasse etter vedkommende stasjons ytelse uavhengig av spenningsnivå. Men i de tilfeller hvor koblingsanlegget er viktigst skal dette klassifiseres som koblingsstasjon, og gis klasse etter spenningsnivå (se under).

En del koblingsanlegg, som opprinnelig tilhørte en kraftstasjon og var klassifisert sammen med denne, er i dag blitt så viktige i nettet (f. eks. 3-veis koblingsstasjon) at de nå må klassifiseres som egne koblingsstasjoner (se under) og gis klasse etter det nettnivået de er en del av. Men det vil ikke ha betydning for klassifiseringen av selve kraftstasjonen eller dennes nettilknytning som uansett klassifiseres etter sin generatorytelse.

Frittstående koblingsstasjoner klassifiseres som selvstendige anlegg etter spenningsnivå. Som koblingsstasjon regnes som regel et fullverdig anlegg med samleskinne, brytere og felt for flere avganger for kraftledninger.

Enkeltbrytere, T-avgreninger og lignende regnes ikke som egen koblingsstasjon, men som del av vedkommende kraftledning, eventuelt den kraftstasjon som er tilknyttet. Etter forskriften blir spenningsnivå for disse lagt til grunn for klasse, og de vil få samme klasse som tilknyttede kraftledninger.

Kraftledning (avgrening med tilhørende brytere, muffer og lignende) for innmating av kraft fra kraftstasjon eller radial ut til transformatorstasjon, sentralnettskunde eller lignende får klasse etter vedkommende stasjon som er tilknyttet.

Lokalkontrollanlegg og annet som funksjonelt er en del av en kraft-, transformator eller omformerstasjon, klassifiseres etter vedkommende stasjons klasse. Men komponenter og anleggsdeler som har betydning for hele eller deler av driftskontrollsystemet for øvrig som drift mv. av andre anlegg, klassifiseres og sikres etter driftkontrollsystemets klasse.

5.2.9 Energianlegg for rene industriformål mv.

Nettanlegg som for eksempel transformatorer, omformere (likerettere), kraftledning, samt fjernvarmeanlegg som eies av virksomheten selv for egne formål og hvor det ikke er andre sluttbrukere av betydning, klassifiseres ikke etter denne bestemmelsen, men kan fremdeles bli klassifisert ved enkeltvedtak – jf. § 5-7.

Alle kraftstasjoner med en samlet generatorytelse på minst 25 MVA som fysisk kan levere elektrisk kraft på ordinært (samkjørt) nett, skal klassifiseres og vedkommende (drifts-) enhet skal være med i KBO.

5.2.10 Klassifisering av midlertidige energianlegg og løsninger

I forbindelse med blant annet nett- og kraftutbygginger kan det oppstå behov for å etablere midlertidige løsninger. Det kan for eksempel omfatte midlertidige tilkoblinger eller mellomtransformering mellom eksisterende og framtidig spenning. I slike tilfeller

kan det for et avgrenset tidsrom aksepteres at slike anlegg eller anleggsdeler ikke klassifiseres eller sikres etter dette kapitlet. Normalt settes en øvre grense for midlertidige løsninger ved 10 år. Det forutsettes at det foreligger konkrete planer for utbygging eller oppgraderinger. Tvilstilfeller avgjøres av NVE.

Der hvor for eksempel transformatorer med tilhørende arrangementer inngår i midlertidige løsninger i forbindelse med konkrete planer for nettutvikling med ombygging fra et spenningsnivå til et annet, kan slike transformatorer også unntas fra å medregnes i ytelsesgrunnlaget for klassifiseringen. Sikringstiltakene ved slike transformatorer kan utføres tilsvarende mer moderat. Det kan for eksempel aksepteres at det ikke etableres transformatorcelle for transformator som ikke blir en del av det framtidig permanente anlegget.

Når anlegget/anleggsdelen ferdigstilles og kan anses for permanent, skal dette uoppfordret sikres etter den klasse det da får ifølge bestemmelsene i dette kapitlet.

5.2.11 Klassifisering etter ytelse og hva som medregnes

Dette leddet omfatter ytelseskriteriene for det enkelte anlegg og klasse, hvilke komponenter som skal medregnes og hvordan det skal regnes.

For å ha et enkelt og kontrollerbart mål, er klassifiseringskriteriene fastsatt på grunnlag av merkeytelse på de installerte generatorene, transformatorene, kjelene og varmevekslerne. Den faktiske eller gjennomsnittlige ytelse, hva som er angitt i konsesjonen, eller ved for eksempel midlertidig drift på lavere spenningsnivå, er uten betydning. Unntak kan gjøres dersom det foreligger åpenbare og varige urimeligheter.

Spenningsnivået angis i runde tall og skal i praksis forstås som den maksimale spenningen som anlegget er beregnet for.

For kraftstasjoner regnes samlet generatorytelse. Dette gjelder også om generatorene står plassert i ulike deler av en stasjonsbygning eller stasjonen er oppdelt i flere fjellhaller eller turbinene har ulike tilløpsrør, så lenge det funksjonelt må regnes for en stasjon. Fysisk helt separate anlegg som for eksempel utnytter og er plassert i forhold til ulike fallhøyder, skal derimot normalt regnes hver for seg. Det samme gjelder om det bygges en helt ny stasjon (for eksempel i fjell) og den eldre ligger i dagen. Normalt opprettholdes den tidligere vedtatte kraftstasjonsinndelingen, selv om kraftstasjonen(e) nå klassifiseres etter denne paragrafen. Rene generatortransformatorer medregnes ikke i ytelsen – se neste punkt.

For transformatorstasjoner er det hoved-(kraft-)transformatorene mellom ulike spenningsnivåer i nettet som skal medregnes, det vil si ikke de rene generatortransformatorene eller transformering for reguleringstekniske formål (fasekompensering, spoler, spenningsregulering og lignende). Heller ikke mobile reserve-/beredskapstransformatorer eller midlertidig oppsatte transformatorer regnes med. For transformatorer med flere funksjoner (viklinger) regnes høyeste ytelse av transformering mellom nettnivåer. For generatortransformatorer som også transformerer mellom ulike spenningsnivåer i nettet (f.eks. treviklinger) eller som leverer direkte til lokal forsyning (for eksempel 11 kV) medregnes ytelsen mot nettet.

For transformatorstasjoner i klasse 2 og 3 brukes på denne måten både ytelse og spenning for å skille funksjoner i de ulike nettnivåene fra hverandre.

5.2.12 Kommentarer til de enkelte klasser

5.2.12.1 Klasse 1

Bokstav a, kraftstasjon:

Energiloven (før vedtak i 2012) fastsatte med virkning fra 1991 en nedre grense på 15 MVA for når det normalt kunne stilles krav til sikringstiltak. For å følge utviklingen i kraftsystemet siden forrige endring, er nedre grense nå oppjustert til en ytelse på 25 MVA uansett spenning/nettnivå.

Bokstav b, transformatorstasjon:

For transformatorstasjoner har vi beholdt den samme nedre grensen på 10 MVA, som tidligere var fastsatt i *energiloven* (før vedtak i 2012). Denne grense er satt slik for at all vesentlig transformering mellom regional- og høyspenningsfordelingsnett, fremdeles skal bli klassifisert.

Bokstav c, omformerstasjon:

For omformeranlegg er nedre grense nå hevet til 10 MVA, og er samme som for transformatorstasjoner. Det betyr i praksis at bestemmelsen ikke lenger omfatter omforming av elektrisk kraft for jernbane og sporveisdrift.

Bokstav e, selvstendig koblingsstasjon:

Denne bestemmelse omfatter kraftledninger i høyspenningsfordelingsnettet, men ikke de tilhørende nettstasjonene.

Bokstav f, fjernvarmesentral:

Grensen for klassifiserte fjernvarmesentraler blir av hensyn til vesentlighet hevet betydelig i forhold til den nedre grense på 10 MW i *energiloven* (før vedtak i 2012). Grensen gjelder installert ytelse i selve fjernvarmesentralen og inkluderer også eksternt tilført energi fra for eksempel søppelforbrenningsanlegg og varmepumper.

5.2.12.2 Klasse 2

Bokstav a, kraftstasjon:

For kraftstasjoner er grensen på 100 MVA hevet i forhold til tidligere praksis. En rekke eldre/ mindre kraftstasjoner går fra klasse 2 til klasse 1, og antall kraftstasjoner i klasse 2 blir vesentlig redusert selv om mange anlegg i klasse 3 nå blir klasse 2.

Bokstav b, transformatorstasjon:

For transformatorstasjoner skal grensen på 50 MVA omfatte viktig transformering i regionalnettet og er i tråd med dagens praksis.

Bokstav c, omformerstasjon:

For omformerstasjoner/-anlegg settes grensen maksimalt i klasse 2.

Bokstav d, selvstendig koblingsstasjon og e, kraftledning:

Disse omfatter i prinsippet dagens regionalnett. For sentralnettsanlegg som bygges eller drives for 132 kV, kan det fattes enkeltvedtak om klasse 3 – se § 5-7.

Grensen på 30 kV for ledning er valgt for å skille mellom lokal fordeling opp til 24 kV og for regionalnett fra rundt 33 kV og oppover.

Bokstav f, fjernvarmesentral:

Fjernvarmesentral i klasse 2 vil bare gjelde et fåtall. Det er ikke forskriftsfestet fjernvarmesentraler i klasse 3.

5.2.12.3 Klasse 3

Bokstav a, kraftstasjon:

Her er grensen satt ut fra nødvendigheten av å kunne opprettholde viktig produksjonskapasitet i sentralnettet i ekstraordinære situasjoner. Kraftstasjoner lagt i fjell er en vesentlig del av sikringen. Kraftstasjoner på minst 250 MVA som ikke er plassert i fjell, vil være i klasse 2.

Bokstav b, transformatorstasjon:

For transformatorstasjoner i klasse 3 er det satt en grense på større enn 100 MVA. Dette skyldes at en del stasjoner som tidligere var og fremdeles bør være klassifisert i klasse 2, har akkurat denne ytelse. Vi vil heller foreta en individuell vurdering av grensetilfellene mellom klasse 2 og 3. For en del ytelsesmessig mindre, men viktige anlegg vil den tidligere klasse 3 bli opprettholdt ved enkeltvedtak etter § 5-7.

Videre er det her innført en del spenningsmessige avgrensninger for transformatorer som transformerer mellom ulike spenningsnivå på samme nettnivå. For eksempel skal stasjoner som kun transformerer mellom 132 og 50 kV i regionalnettet (inntil 200 kV) normalt ikke gi en stasjon med høyere klasse enn klasse 2 uansett ytelse. Tilsvarende vil stasjoner som kun transformerer fra regional- til lokalnettet (< 30 kV) i utgangspunktet ikke få høyere klasse enn klasse 2 uansett ytelse. Men også her kan NVE gjøre unntak ved enkeltvedtak etter § 5-7 for særlig viktige forsyningsområder.

§ 5-3. Sikring av klassifiserte anlegg

Alle klassifiserte anlegg skal prosjekteres, plasseres, utføres, utrustes, sikres, driftes og holdes i slik stand at risiko for skade, havari og funksjonssvikt og andre uønskede hendelser og handlinger blir minst mulig.

5.3.1 Hensikten med bestemmelsen

Hensikten med denne bestemmelsen er blant annet å stille krav til en hensiktsmessig prosess, slik at sikringsnivå og sikringstiltak blir en del av anleggets utforming og utførelse. Dette gjelder helt fra stedsvalg foretas og prosjekteringen starter, og fram til anlegget er i drift med oppfølgende kontroll og vedlikehold. Krav til sikring og andre beredskapshensyn blir langt på vei en del av konsesjonsprosessen. Det vises her også til gjeldende utgave av NVEs *Veileder for utforming av søknad om anleggskonsesjon for kraftoverføringsanlegg*.

Anleggets sikringsmessige prosjektering, utførelse og tilstand mv. etter denne bestemmelsen skal kunne dokumenteres etter forskriftens § 2-10 Internkontrollsystem.

I de etterfølgende §§ 5-4 til 5-6 om sikringstiltak for anlegg klasse 1 til 3, er de tidligere funksjonskravene i BfK til sikringstiltak og nivå etter klasse videreført uten større

endringer. I tillegg er en del vesentlige tiltak som i dag er angitt i veiledningen, blitt forskriftskrav. I forskriften har vi funnet det redaksjonelt mest hensiktsmessig å samle disse i et vedlegg for hver klasse.

I denne veiledningen har vi valgt å inndeले sikringstiltakene etter tema (romertall I til X) og deretter anleggenes type og klasse.

§§ 5-4, 5-5 og 5-6. Sikringstiltak for klasse klasse 1-3

§ 5-4. Sikringstiltak for klasse 1

Anlegg klassifisert i klasse 1 skal, i tillegg til kravene til sikring etter §§ 5-1 og 5-3, oppfylle følgende generelle krav til sikring:

Anlegget skal utføres etter krav til normalt sikringsnivå, som nærmere angitt i vedlegg 1.

Skader og funksjonstap skal oppdages innen rimelig tid.

Skader skal utbedres og anleggets funksjoner skal gjenopprettes uten ugrunnet opphold.

Anlegg klassifisert i klasse 1 skal også oppfylle særlige krav til sikring for sin klasse og anleggstype som fastsatt i vedlegg 1, jf vedlegg 4.

Vedlegg 1 står i sin helhet i kapittel 10 i veiledningen.

§ 5-5. Sikringstiltak for klasse 2

Anlegg klassifisert i klasse 2 skal, i tillegg til kravene til sikring etter §§ 5-1 og 5-3, oppfylle følgende generelle krav til sikring:

Anlegget skal utføres og utstyres etter middels høye krav til sikring, som nærmere angitt i vedlegg 2.

Tap av vitale funksjoner skal begrenses og etter eventuell skade skal anleggets funksjonalitet gjenopprettes uten ugrunnet opphold.

Anlegg klassifisert i klasse 2 skal også oppfylle særlige krav til sikring for sin klasse og anleggstype som fastsatt i vedlegg 2, jf vedlegg 4.

Vedlegg 2 står i sin helhet trykt i kapittel 10 i veiledningen.

§ 5-6. Sikringstiltak for klasse 3

Anlegg klassifisert i klasse 3 skal, i tillegg til kravene til sikring etter §§ 5-1 og 5-3, oppfylle følgende generelle krav til sikring:

Anlegget skal utføres og utstyres etter høye krav til sikring, som nærmere angitt i vedlegg 3.

Vitale funksjoner skal opprettholdes i ekstraordinære situasjoner og anleggets funksjonalitet skal gjenopprettes uten ugrunnet opphold.

Anlegg klassifisert i klasse 3 skal også oppfylle særlige krav til sikring for sin klasse og anleggstype som fastsatt i vedlegg 3, jf vedlegg 4.

Vedlegg 3 står i sin helhet trykt i kapittel 10 i veiledningen.

5.4.1 Hensikten med bestemmelsene

Hensikten med bestemmelsene i §§ 5-4, 5-5 og 5-6 er for det første å beskytte energianleggene mot alle uønskede hendelser og handlinger som kan skade eller hindre energiforsyningen, hvor klasseinndelingen tar hensyn til hvert enkelt anleggs betydning. For det andre skal bestemmelsene sikre at forsyningen kan gjenopprettes raskt og effektivt dersom skade eller funksjonshindring likevel skjer.

5.4.2 Inndeling av veiledningen til bestemmelsene

Den videre veiledningen for sikringstiltak for anlegg klasse 1 til 3, følger ikke rekkefølgen i forskriften. I stedet har vi delt den inn i logiske tema, anleggstype og klasse. Disse er nummerert med romertall (I til X). Samlet sett mener vi dette er den mest effektive måten å gi en samlet framstilling av sikringstiltakene på. Samtidig gir det en gjenkjenningseffekt i forhold til det tidligere regelverket.

Til hjelp har vi tatt inn i veiledningen forskriftens mer detaljert krav i vedlegg 1 til 3. Vi understreker likevel at hele forskriften - med de mer overordnede og funksjonelle kravene - må leses i sammenheng. Nummererte punkter som det henvises til, er hentet fra vedleggene. Punkter som starter med 1, står i vedlegg 1 til bfe, de som starter med 2 fra vedlegg 2 osv. Forskriften med vedlegg (1 til 4) står i sin helhet i kapittel 10.

5.4.3 Funksjonelle kriterier, nærmere om hensikten

Sikringstiltakene etter disse bestemmelsene skal:

- Forebygge og forhindre uønskede hendelser og handlinger.
- Øke evnen til å håndtere ekstraordinære situasjoner som oppstår.
- Begrense skadevirkninger og gjenopprette funksjon dersom skade likevel oppstår.
- Uønskede hendelser som det må etableres sikringstiltak mot, er blant annet:
 - Utilsiktete hendelser som kan forårsake tap av vitale funksjoner som for eksempel brann, havarier og teknisk svikt.
 - Naturskade som ras (jord, stein, snø), steinsprang, flom/oversvømmelse, belastninger fra nedbør og uvær, snø, is og atmosfæriske forstyrrelser.
 - Inntrengning av uønskede personer og kjøretøy, urettmessig overtakelse og ytre skadeverk (inkludert håndvåpen, splinter og elektronisk påvirkning som jamming og EMP).
- Krav til sikringstiltak er avhengig av anleggenes klassifisering etter § 5-3, og kravene øker med klasse.

Sikringstiltak består av fire ulike kategorier tiltak:

- Oppdagelse og reaksjon.
- Fysisk sikkerhet i form av ulike barrierer.
- Redundans.

- Gjenopprettingsevne.

Kategoriene utfyller hverandre, og alle fire må derfor alltid være med, i større eller mindre grad. Virksomheten skal kunne dokumentere at kravene i dette kapitlet, er oppfylt samlet sett.

Sikringstiltakene skal, avhengig av anleggets klasse, art, konstruksjon og en lokal risiko- og sårbarhetsanalyse, samlet representere en balansert kombinasjon av tiltak innenfor de ulike kategoriene. Der det synes hensiktsmessig med sikring ut over minimumskravene, kan virksomheten selv kombinere de ulike kategoriene, for eksempel kan mangler i redundans i noen tilfeller kompenseres ved god fysisk sikring eller god gjenopprettingsevne. Denne bestemmelsen gir dermed mulighet for ulike tilpasninger og kombinasjoner av løsninger.

Sikringstiltakene skal samlet sett hindre/begrense skader på anlegg og sikre forsyningssikkerheten, også i ekstraordinære situasjoner.

5.4.3.1 Skallsikring

Med skallsikring forstås beskyttende bygningsmessige konstruksjoner som helt eller delvis omslutter viktige eller sårbare komponenter eller et definert område. Det kan være spesialkonstruksjoner eller bygningskropp inkludert dører, vinduer mv. som er oppført etter visse byggetekniske og sikringsmessige spesifikasjoner.

Skallsikring av vitale komponenter omfatter blant annet kraftstasjoner, lukehus, varmesentraler, krafttransformatorer, kapslede SF₆ koblingsanlegg, omformere, endemuffer og i noen grad driftsbygg (driftssentral, kontrollrom, tele- og nødstrøm) o.l.

5.4.3.2 Områdesikring

Med områdesikring forstås anleggets ytre sikringssone. Det består av barrierer som markerer anleggsgrensen for uvedkommende, og som fysisk skal hindre eller begrense atkomsten til anlegget eller frittstående anleggsdeler.

5.4.3.3 Rømningsveier

Vi forutsetter at kravet til rømningsveier oppfylles, og at disse tilrettelegges og utføres på en slik måte at de ikke er til hinder for oppfyllelse av andre sikringstiltak – for eksempel at:

- Avstengte/ avlåste anleggsdeler må kunne åpnes når det er personell til stede i anlegget.
- Innvendige åpningsanordninger ikke må kunne åpnes eller manipuleres utenfra.

5.4.4 Nærmere om normer og standarder

Dette kapitlet utdyper innholdet i vedlegg 4 til bfe, som i sin helhet finnes i kapittel 10 i veiledningen.

Hensikten med bruk av normer og standarder er at man på en enkel og dokumenterbar måte kan bestille og få levert produkter og liknende som oppfyller de kravene og anbefalingene til funksjon og sikringsnivå som stilles.

I denne paragrafen om sikringsnivå henviser vi til en del gjeldende normer om brannvern, konstruksjoner og beskyttelse mot inntrengning, først og fremst til den nye europeiske

normen EN som er antatt som norsk standard NS-EN, i denne veiledningen forkortet til EN. Det finnes imidlertid tilnærmet likeverdige normer etter tidligere norsk standard (NS), selv om disse nå er erstattet av NS-EN. Også svensk og internordisk standard er en del brukt på nevnte områder. De nordiske forsikringsforbundene har med tanke på blant annet innbruddssikring med videre utarbeidet en "Sammenligningsnøkkel". Denne med forklaring til normer for sikring og sikkerhet finnes på nettsidene til "Forsikringsselskapenes Godkjennelsesnemnd (FG): [<http://fg.fnh.no/>]. Også Direktoratet for samfunnssikkerhet og beredskap henviser til ulike relevante normer i sitt regelverk og publikasjoner [<http://www.dsb.no/>].

Formålet med henvisningen til standarder er å vise hvor nivået skal ligge for ulike produkter. Likeverdige produkter som oppfyller de nevnte normene, kan godtas.

For låsesystemer viser vi også til "Forsikringsselskapenes Godkjennelsesnemnd" (FG), godkjenningsklasse.

For elektroniske/ elektromekaniske låsesystem har FG (se <http://fg.fnh.no/>) utgitt en publikasjon med krav til slike. Disse er inndelt i 3 beskyttelsesklasser hvorav B2 og B3 har mekanisk tilleggslås. Både av hensyn til inntrengingssikkerhet og egen tilgjengelighet til bygg og anlegg, er det B2 og B3 som er relevante for energiforsyningen; B3 for anlegg i klasse 3.

I det etterfølgende er krav og anbefalinger til utførelse av dette differensiert etter anleggenes klasse. Europeisk norm EN 1627 (dører, vinduer med mer) og EN 12320 (hengelåser med mer) er her brukt som eksempler. Det finnes tilsvarende EN-normer for blant annet faste låser, låskasser med videre, og vindusglass.

De fleste sikringsstandarder (for eksempel mot innbrudd) etter EN har skala fra sikringsklasse 1 til 6. Denne veiledningen starter på sikringsklasse 2 som for eksempel for en entrèdør (leilighet) tilsvarer normal innbruddssikring etter EN 1627. Tilsvarende starter veiledning på FG i klasse 2, siden FG-klasse 1 er beregnet for "redskapsboder" og liknende.

Mer utfyllende informasjon om gjeldende og eldre standarder er gitt i tabeller i vedlegg 11 til denne veiledningen.

Se for øvrig også veiledning til § 8-9 Forholdet til eldre vedtak om klassifisering og overgangsregler som beskriver hvordan NVE vil praktisere forskriftens bestemmelser om sikringstiltak for henholdsvis nye energiforsyningsanlegg, eksisterende anlegg som skal bygges om, eller utvides, og øvrige eksisterende anlegg.

5.4.1 Krav til sikringsnivå

Forskriften omfatter sikringsnivå med betegnelser som normal, middels, god og høy. Nedenfor angir vi hva dette innebærer og hva som anses som et minstekrav til å oppfylle forskriftens bestemmelser, med henvisning til normer i NS-EN i vedlegg 4 til bfe.

Eksempel: For krav til sikring mot innbrudd og inntrengning – er relevante normer EN 1627, EN 1303, EN 12209 og EN12320. Disse har seks sikringsklasser på en stigende skala fra en til seks.

Sammenhengen mellom kategoriene for sikringsnivå i forskriften har følgende sammenheng med skalaen for sikringsklasser:

- Sikringsklasse 1 (eller ingen) aksepteres ikke.
- Med ”normal” menes sikringsklasse 2 eller bedre.
- Med ”middels” menes sikringsklasse 3 eller bedre.
- Med ”god” menes sikringsklasse 4 eller bedre.
- Med ”høy” menes sikringsklasse 5 eller 6.

Tilsvarende for FG klasser - en til fem - med en litt annen skala. Også her vil klasse 2 være et absolutt minimum.

En nærmere oversikt (tabell) over sammenhengen mellom ulike sikringsklasser er gitt i vedlegg 11 til veiledningen.

Tilsvarende brannklassifisering/-motstand i minutter etter EN 13501

EI 30 – 60 – 90 – 120 – 180 – 240

Her med den forskjell at dersom normal byggestandard (for eksempel branncelle) etter forskriftene til *plan- og bygningsloven (pbl)* tilsier EI 30 danner dette minimum for bfe sine krav til ”normal”, og den videre skala blir med dette som utgangspunkt. Om kravet etter *plan- og bygningsloven* derimot er EI 60, blir bfe sine krav å regne ut fra dette osv. Likevel er det slik at kravene etter bfe kan tilpasse byggets konstruksjon og øvrig brannsikring.

Dette er nærmere angitt under de enkelte anlegg og klasser i etterfølgende veiledning om fysiske sikringsiltak etter anleggstype og klasse. Merk at punkter som det henviser i teksten i tabeller er hentet fra vedlegg 1-3 til bfe.

For en sammenstilling av sammenhenger mellom sikringsnivå etter denne forskrift kapittel 5 og sikringsklasser etter europeiske normer (NS-EN) med videre for ulike elementer i en balansert sikring, se vedlegg 12.

Del I Fysisk utførelse - beskyttelse

5.1.1 Generelt – alle anlegg

Denne delen vektlegger fysisk sikring av viktige anleggsdeler. Angitte dimensjoner, kvaliteter med videre gir ulike minimum av sikringsnivå for å beskytte anleggsdelene mot et utvalg av dimensjonerende hendelser og handlinger, men tar ikke alltid hensyn til konstruksjonsmessige og liknede krav. Det forutsettes derfor at bygnings-, brann- og elektrotekniske krav til bygninger, øvrige konstruksjoner og elektriske komponenter beregnes og utføres etter gjeldende regler og normer. Dette kan resultere i økte, men ikke reduserte krav til konstruksjon og utførelse.

Alle deler av anlegget med tilhørende konstruksjoner og sikringstiltak skal tåle alle de påregnelige fysiske og elektriske belastninger de kan bli utsatt for både under normale og ekstraordinære forhold. Det skal tas særlig hensyn til at beskyttelsen skal utgjøre en sikringsmessig helhet i forhold til havarier, ulykker, inntrengning, beskytning og andre risikoer, etter § 5-8 Analyse.

Eksempel på tiltak mot hendelse/handling av dimensjonerende betydning:

Konstruksjonen må ha evne til å motstå treff av et tungt kjøretøy/anleggsmaskin med etter forholdene høy fart, enten ved ulykke eller som bevisst inntrengning/skadeverk.

For valgte konstruksjoner bør alle relevante krav etter EN-normer, blant annet EN 1992 (tidligere NS 3473), oppfylles for dimensjonering, utførelse og holdbarhet.

Ved prosjektering og utførelse bør pålitelighetsklasse 3 etter EN 1990 (tidligere NS 3490) følges.

Fordi energiforsyningsanlegg har lang levetid, bør det velges høy holdbarhet i form av korrosjonsbeskyttelse (syrefasthet) av metall og impregnert treverk. Det bør velges betong av god fasthetsklasse, og bestandighetsklasse, og brukes god overdekning over armering. Forhold som vær og forurensning kan gjøre det gunstig å velge dimensjoner og kvaliteter utover det selve beskyttelsesbehovet tilsier.

Det forutsettes at gjeldende krav til helse, miljø og sikkerhet (HMS) ivaretas. Blant annet må krav til rømningsveier oppfylles. Rømningsveier må altså tilrettelegges og utføres slik at oppfyllelse av beredskapsforskriftens krav til sikringstiltak ikke er til hinder. F.eks. kan normalt avstengte/ avlåste adkomster åpnes når det er personell til stede. Det kan monteres innvendige åpningsanordninger på beskyttende dører og liknende, men disse må ikke kunne åpnes eller manipuleres utenfra – se også nærmere veiledning om rømningsveier over.

I daglig drift skal viktige anlegg være sikret på et nivå som tilsvarer god industrisikkerhet/ standard for forebygging og mottiltak ved innbrudd, hærverk, enkle forsøk på sabotasje, brann, teknisk svikt eller naturgitt skade.

En del av hensikten med disse bestemmelsene er å hindre at uvedkommende får anledning til å utføre tilsiktede handlinger rettet mot energiforsyningen. Denne forskriften kan derfor stille strengere krav, men aldri lavere krav enn DSBs bestemmelser om elsikkerhet.

I en beredskapssituasjon skal det være supplerende sikrings- og beredskapstiltak som styrker beskyttelsen av vitale installasjoner og anleggsdeler mot for eksempel sabotasje. Dette kan skje ved erklært beredskap, vedtak/varsel fra NVE, eller når virksomheten selv vurderer dette som relevant eller nødvendig.

Valg av sikringstiltak i henhold til klassebaserte krav utformes etter anleggets art og omgivelser. Enkelte krav (se nedenfor) er uavhengig av slike forhold.

Når det gjelder plassering av nye energiforsyningsanlegg, må virksomheten i sin risikovurdering vektlegge blant annet utsatthet for naturgitt skade, nærhet til utsatte objekter (storulykkepotensialet, risiko for transportulykker, tilgang ved reparasjon etc.). Dette er også forhold som skal vurderes i forbindelse med konsesjonssøknader. Se for øvrig NVEs veiledere for søknad om konsesjon etter *energiloen*, som *Veileder for utforming av søknad om anleggskonsesjon for kraftoverføringsanlegg*, *Konsesjonshandsaming av vasskraftsakar*, *Rettleiar for utarbeiding av meldingar*, *konsekvensutgreiingar og søknader*, *Veileder i utforming av konsesjonssøknader for*

vindkraftverk ≤ 10 MW og NVEs veileder Utforming av konsesjonssøknad for fjernvarmeanlegg .

Nedenfor beskriver vi nærmere kravene til de enkelte typer av anlegg og klasser.

Virksomheten kan finne alternative måter å løse kravet på, men dette må kunne dokumenteres. Eventuelle unntak, for eksempel ved at dette ikke passer for et gitt anlegg, skal begrunnes og dokumenteres.

5.1.2 Forebygge og forhindre tap av funksjon og ødeleggelse - funksjonelle krav til anlegg i klasse 1

§ 5-4. Anlegg klassifisert i klasse 1 skal, i tillegg til kravene til sikring etter § 5-1 og § 5-3, oppfylle følgende generelle krav til sikring:

1. Anlegget skal utføres etter krav til normalt sikringsnivå, som nærmere angitt i vedlegg 1.

For anlegg i klasse 1 gjelder krav til solid bygg (skallsikring) etter normal god byggestandard og eventuelt inngjerding (områdesikring – se under) dersom det er ytre anleggsdeler (friluftsanlegg, lagerbygg og lignende). Disse må minst sikres etter normale krav til norm for sikringsklasse. Etter FG blir dette klasse 2 eller 3. Etter for eksempel EN 1627 og EN 12320 blir dette sikringsklasse 3 eller 4.

5.1.3 Forebygge og forhindre tap av funksjon og ødeleggelse - funksjonelle krav til anlegg i klasse 2

2.1. For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:

- 2.1.1 b. Fysisk og elektrisk utførelse og beskyttelse skal være på et nivå som begrenser tap av funksjon og ødeleggelse.

5.1.4 Forebygge og forhindre tap av funksjon og ødeleggelse - funksjonelle krav til anlegg i klasse 3

3.1 For transformatorstasjoner, koblingsanlegg/-stasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:

- 3.1.1 b. Fysisk og elektrisk utførelse og beskyttelse skal være på et nivå som forebygger eller forhindrer tap av funksjon og ødeleggelse.

5.1.5 Nærmere om ulike sikringstiltak

For anlegg i klasse 2 og 3 gjelder krav til **områdesikring, skallsikring og sonesikring**. Disse skal gi fysisk beskyttelse (barrierer) mot uønskede hendelser og handlinger både utvendig (f.eks. forsøk på inntrengning og innvendig (f.eks. brann og eksplosjoner).

For en del anlegg i byer og lignende områder med begrenset plass vil det ikke være mulig å utføre tilfredsstillende områdesikring. I slike tilfeller må man ta hensyn til dette ved utforming og gjennomføring av skallsikringen hvor eventuelle ekstra tiltak må vurderes.

5.1.5.1 Skallsikring

Skallsikring omfatter blant annet bygningskropp, transformatorceller med stengsler, ståldører og rister, kraftverksport (stål). Det må bygges og sikres etter middels eller høye krav til standard/norm for sikringsklasse, alt etter klasse og lokal risikovurdering. Det må rettes særlig oppmerksomhet mot svake punkter som vinduer, dører, kabelføringer og andre mulige atkomster.

5.1.5.2 Sonesikring

Sonesikring omfatter særlige viktige områder/rom som kontrollrom, prosessmaskin/sambandsrom, nødstrøm og liknende. Sikringsnivå tilpasses klassen, viktigheten av utstyret i sonen, og nivået på den ytre skallsikringen.

Tilpasningen av sikringsnivået på sonesikringen skal skje ved at jo svakere skallsikring det er, desto bedre må sonesikringen være.

5.1.5.3 Områdesikring

Områdesikring (også kalt perimetersikring) omfatter for eksempel bommer, gjerder, porter med låser og beslag, eventuelt betongskillere og store stein. Anleggene sikres etter relevante middels høye krav til standard/norm for sikringsklasse. Etter FG blir dette 2 eller 3. Etter EN 1627 og EN 12320 blir dette sikringsklasse 3 eller 4.

- Låser med tilhørende beslag og innfesting må for klasse 2-anlegg minst tilsvare FG klasse 2 med tilsvarende soliditet i port, bom og liknende i en balansert helhet, uten glipper og svake punkter.
- Ofte vil for eksempel en transformator i klasse 2 stå i tett urban bebyggelse, og det kan da være umulig eller lite ønskelig eller hensiktsmessig å etablere fullverdig områdesikring. I tettbebygde områder, eller når andre særlige hensyn tilsier det, kan områdesikringen tillempes, men må da kompenseres ved andre tiltak (bedre skallsikring og liknende).
- Ved kraftstasjon klasse 2 vil det være naturlig å sette opp veibom og liknende, men det er ikke noe krav at portalbygg og liknende skal gjerdes inn dersom skallsikringen er tilfredsstillende.
- Alle energiforsyningsanlegg i klasse 3 skal ha effektiv omsluttende områdesikring rundt viktige anleggsdeler, hvis ikke særlige forhold i omgivelsene tilsier noe annet.
- **Bommer.** Der forholdene tilsier dette, skal kjøreatkomster sikres med solid veibom i passe avstand fra kjøreport. Bommen bør kunne låses med lås og beslag i sikringsklasse 3 eller 4. Omkjøring av bom vanskeligjøres med grøfting eller kjøretøyavvisere.
- **Gjerder.** Gjerder må være høye og solide. Høyden på gjerdet bør være på minst 2,7 meter og i tillegg til nevnte høyde skal det alltid vurderes en anretning på toppen av gjerdet som ytterligere forebygger og forhindrer uønsket adkomst til området, som for eksempel piggtråd. Gjerdet (stolpene) må være solid fundamentert, støpt eller liknende i løs grunn, nedboret i fjell. De må utstyres med solid og stram topp og bunntråd, eventuelt vinkeljern eller liknende, godt festet i stolpene. Gjerdedukens maskevidde (flettverksduk) skal maksimalt være

50 millimeter og tråddykkelse minimum 2,8 millimeter. Gjerdeduken må være godt festet i både topp-/ bunntråd og i gjerdestolpene, både med tilstrekkelig antall og solide festetråder. Alle skjøter i gjerdetråd og duk må være godt sikret/sammenføyd. Glipper i/under gjerdet må ikke forekomme. Gjerdet utføres evt. som stålstendere eller strekkmetall.

- **Gjerdeporter.** Gjerdeporter (gang og kjøre/transport) må være solide med høyde og utførelse minst like bra som gjerdet. Stolper må støpes i løs grunn, bores ned eller boltes i fjell. Glipper må være minimale. Kjøreporter som skal beskytte kjøreatkomst mot innbrudd og inntrengning fra kjøretøy, gis solid utførelse. To-fløyede porter må ha låsbar midtsikring mot bakke.
- Styresystemet til elektrisk eller liknende drevne, eventuelt fjernstyrte porter må ikke kunne manipuleres utenfra eller via åpninger i port eller gjerde. Disse må også låses mekanisk (se under).
- Portene må være utstyrt med låser og beslag i sikringsklasse 3 eller 4, og bakkantbeslag eller hengsler sikret mot avløfting.
- Der forholdene tillater dette, bør områdesikring settes opp i en avstand på minst 30 meter ("kasteavstand") fra vitale komponenter.
- Alle elementer i områdesikringen bør holdes fri for vegetasjon, bygningselementer og andre gjenstander i en sone på 3 meter til alle kanter.
- Alle løse gjenstander (for eksempel stiger, søppeldunker, kabeltromler, hengere) som kan medvirke til enkel forsering av områdesikringen skal normalt være plassert på innsiden, helst ute av syne, innelåst (alle verdigjenstander) eller fastlåst.
- Alle monterings-elementer (eksempelvis låser, beslag, bolter, skruer) skal være sikret mot enkel demontering (av-/oppskruing).

Utover dette må virksomheten gjennomføre ytterligere tiltak ut fra stedlige forhold og risiko. Ulike tiltak utføres hvor det foreligger en forhøyet risiko.

5.1.5.4 Permanent tilleggssikring

Eksempler på permanent tilleggssikring:

- Gjerdet forsterkes eller bygges høyere på grunn av anleggets utforming, snødybder, terreng, vegetasjon og omgivelser for øvrig.
- Øvrige elementer som stolper, topp, bunn og innfesting forsterkes tilsvarende.
- Montering av deteksjonsutstyr/-alarmer i ulike atkomster og innvendige rom. Forsterket overvåkning av funksjoner.
- Forsterkning av gjerder og porter, bommer i kjøreatkomst og bakveier og om nødvendig supplert med permanente stengsler/hindre som betongskillere eller store stein, forsterkede låser og beslag (høyere FG/sikringsklasse).

- Ekstra krav til dører og porter, kraftverksdør/ kraftverkspport, ekstra kraftverkspport, innbruddssikre vinduer og liknende, ekstra sikring av kabel og ventilasjonssjakter.
- Skuddhemmende glass i kontrollrom, intern dublering av viktige funksjoner så som samband, nødstrøm og andre funksjoner.
- For sonesikring – høyere sikringsklasse på dører, låser mv. eller ekstra brannsikring.
- Ekstra inngjerding av vitale komponenter.

KBO-enheten har ansvaret etter § 5-8 Analyse for å gjennomføre lokale analyser slik at det blir et balansert og helhetlig sikringsnivå tilpasset anlegget.

5.1.5.5 Forberedt tilleggssikring

Forberedt tilleggssikring må raskt kunne iverksettes ved behov. I en beredskapssituasjon må det for eksempel være supplerende sikrings- og beredskapstiltak som styrker beskyttelsen av vitale installasjoner og anleggsdeler mot for eksempel sabotasje. Dette kan skje ved varsel fra NVE eller på enhetens eget initiativ ved en akutt situasjon.

Forberedt tilleggssikring skal være beskrevet i en beredskapsplan og regelmessig testes ut/øves.

Eksempler på planlagte og forberedte sikringstiltak:

- Ekstra bemanning, forsterket vakthold, hyppigere inspeksjoner, ekstra låser og innskjerpede krav til tilgjengelighet og utrykningstider for personell.
- Reparasjonsberedskap gjennomgå, materiell klargjøres og suppleres.
- For fysisk områdesikring – porter forsynes med ekstra/dobbel lås, kjøreatkomster sperres med betongskillere, store steiner eller liknende, ekstra lyskastere settes ut. Kjetting med hengelås, begge i FG klasse 3 eller 4 for dobbel sikring av porter o. l. Kjøretøyavviser (stein, betong).
- For skallsikring – ekstra ståldører låses, stållemmer/skodder for vinduer i for eksempel kontrollrom monteres/lukkes og låses, ekstra kraftverkspporter låses, bjelkestengsel legges på plass.
- Visuell avskjerming av vitale komponenter.
- Ekstra opplysning av områder eller lyskastere over området (observere og blende).
- Anmodning om bistand fra politi mv.
- Energiforsyningsanlegg som er prioritert for forsvarsmessig vakthold, klargjøres for dette, se § 5-10 Vakthold.

Bruk av belysning må vurderes nøye i forhold til situasjon og trussel. I noen tilfeller kan opplysning av selve anlegget virke avskrekkende og gi mulighet for å holde det under oppsikt. I andre tilfeller vil dette eksponere anlegget og blende en selv (omgivelsen blir kun en mørk vegg). I noen tilfeller er det gunstig å mørklegge anlegget og eventuelt vende lyskastere utover for å se og blende omgivelsene (se uten å bli sett).

I det etterfølgende følger nærmere angitte krav til fysisk sikring – beskyttelsesnivå etter klasse og anleggstype.

5.1.6 Spesifikke krav til fysisk sikring - klasse 1

1.1	<i>For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg gjelder følgende krav:</i>
1.1.1	Det skal etableres en adgangskontrollert sone som omfatter alle adkomster til anlegget. Fysisk sikring skal som et minimum omfatte et solid bygg med dører/porter, vinduer og øvrige adkomster. Disse skal oppfylle krav til normalt sikringsnivå etter fastsatte normer.
1.1.2	Brannsikring skal oppfylle krav i henhold til andre relevante forskrifter og normal brannmotstand etter fastsatt norm.
1.1.3	Rom for lokal driftskontroll, styring og samband skal være egne adgangskontrollerte soner, og skal oppfylle krav til normalt sikringsnivå og brannmotstand etter fastsatte normer.

5.1.7 Spesifikke krav til sikring av transformatorstasjon, koblingsstasjon mv. - klasse 1

Alle permanente installasjoner skal ha fysisk beskyttelse (skallsikring), minimum i form av et låsbart lettbygg (elementer, plater eller liknende) som bør oppfylle sikkerhetsklasse 3 etter europeisk standard (EN) normer.

Alle utvendige dører, porter og andre mulige adkomster bør sikres etter sikkerhetsklasse 3 etter gjeldende EN-normer og tilsvarende låseanordninger i FG (Forsikringsselskapenes godkjenningnemnd) klasse 2 eller bedre.

Hærverkshemmende vinduer i klasse P4A eller P5A etter EN 356, eller andre måter å beskytte vinduer og andre mulige adkomster på.

Brannsikring etter veiledningen til *forskrift om elektriske forsyningsanlegg (FEF)* § 4-9 Sikkerhetstiltak og sikkerhetsutstyr, eller bedre. Man skal vurdere å innføre tilleggssikring i forhold til egne akseptkriterier og ut fra analyse av anleggets betydning og lokal risiko. Dette kan eksempelvis være tiltak som gjelder for grunnsikring transformatorstasjon klasse 2.

5.1.8 Spesifikke krav til sikring av transformatorstasjon, koblingsstasjon mv. i klasse 2 og 3

Alle permanente krafttransformatorer skal ha god fysisk sideveis beskyttelse fra alle kanter, ved plassering i fjellrom, fjellskjæring eller liknende, frittliggende oppført celle ("konstruksjon") eller kombinasjoner av dette. Av hensyn til kjøling og utføring av luftledning tillates åpning i konstruksjonens topp.

Det etterfølgende gjelder transformatorstasjoner hvor transformatorene helt eller delvis er plassert i dagen. For transformatorer i fjellrom, se veiledning under om kraftstasjon i fjell.

For gassisolert koblingsanlegg, se eget punkt om dette.

5.1.9 Spesifikke krav til sikring av transformator-, koblingsstasjon mv. - klasse 2

5.1.9.1 Skallsikring - transformatorer

2.2.4 Alle hovedtransformatorer med tilhørende adkomster skal sikres fra alle kanter med bygg eller lignende, med god beskyttelse etter fastsatte normer for sikring og brannmotstand.

Fysisk utførelse/beskyttelse av transformatorer utføres som følger:

- Plasseres i fjellskjæring eller i konstruksjon som gir sideveis beskyttelse fra alle kanter.
- Seksjonering mellom hver enkelt transformator.
- Transformatoren til og med topp endemuffer bør så langt som mulig gis skjul og dekning sett fra omgivelsene. Dekningen kan bestå av fjell (fast terreng) eller av en konstruksjon.
- Konstruksjonen kan utføres med dekningstykkelse tilsvarende minimum 160 millimeter plastøpt armert betong eller bedre, kvalitet (fasthetsklasse) B 25 eller bedre.

Alternativt kan følgende benyttes:

- Prefabrikkerte armerte betongelementer montert i solid konstruksjon (avstivning, sammenføyning, med mer).
- Ekvivalenter i stål (dekningstykkelse minimum 10 millimeter, stålkvalitet bør oppfylle HB 200 (referert til Hardhet Brinell) eller ekvivalenter i aluminium kan benyttes.

Konstruksjonen bør som et minimum tåle en belastning på 2 kN/m² eller mer fra alle kanter.

Konstruksjon bør utføres/utstyres som følger:

- Dører/porter/låser i sikkerhetsklasse 4 eller bedre etter EN.
- Stål-/aluminiumsgitter av tilsvarende kvalitet i lufteåpninger.
- Stengsler av tilsvarende kvalitet som øvrig konstruksjon (betong, stål eller aluminium) monteres i transportåpning.
- Alle føringer for kabler, rør, kanaler, kulverter, og andre mulige adkomster inn til transformatorcelle, muffehus og liknende sikres tilsvarende.
- Transformatorens lokale betjeningsorgan (for eksempel brytere og tappekran for olje) sikres.
- Vegger i konstruksjon, herunder skillevegger mellom flere transformatorer, utføres minimum i brannklasse REI 90 M (M om relevant), og seksjonerende dører med videre i brannklasse EI 90 eller bedre. Det vises for øvrig til veiledningen til FEF § 4-9 Sikkerhetstiltak og sikkerhetsutstyr.

- Varmer, røyk med mer skal kunne oppdages raskt og varsles.

5.1.9.2 Skallsikring - øvrige anleggsdeler

2.2.2	Viktige anleggsdeler som driftsbygg, innendørs apparatanlegg, muffeanlegg og anlegg for stasjonsstrøm og styring skal ha god skallsikring etter fastsatte normer.
-------	---

Øvrige av stasjonens bygninger og liknende med viktige komponenter/ funksjoner utføres/ utstyres som følger:

- Alle utvendige dører/porter/adkomster sikres mot avløfting og med gode låseanordninger, som et minimum sikkerhetsklasse 4 etter EN, og låser med videre i FG klasse 3 eller bedre.
- Alle føringer for kabler, rør, kanaler, kulverter og andre mulige adkomster sikres tilsvarende.
- Hærverkshemmende, klasse P5A, eller fortrinnsvis innbruddshemmende (klasse P6B) vinduer eller bedre, etter EN 356, i kontrollrom og liknende, og i andre rom som gir videre adgang til viktige deler av anlegget.
- Yttervegger og seksjonerende vegger i brannklasse REI 60 M, dører med videre i EI 60 eller bedre.
- Varmer, røyk, med mer skal kunne oppdages raskt og varsles.

Tilleggssikring vurderes og utføres i henhold til egne akseptkriterier og ut fra analyse av anleggets betydning og lokal risiko. Dette kan eksempelvis være tiltak som gjelder for grunnsikring transformator klasse 3.

For SF₆ isolerte koblingsanlegg - se også eget punkt under.

5.1.9.3 Sonesikring - innvendig av særlige viktige områder

2.2.2	Driftskontrollrom og andre rom for styring og samband skal være egne adgangskontrollerte soner med middels sikringsnivå og brannmotstand etter fastsatte normer.
-------	--

Sonesikring omfatter særlige viktige områder/ rom for lokalkontroll, samband, nødstrøm og liknende. Sikringsnivået skal tilpasses viktigheten av utstyret i sonen og nivået på den ytre skallsikringen, normalt minst FG-klasse 3 eller sikringsklasse 3 eller 4 etter EN 1627.

5.1.9 Spesifikke krav til sikring av transformator-, koblingsstasjon - mv. klasse 3

5.1.9.1 Områdesikring

3.2	<i>For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i over nevnte punkt 3.1:</i>
3.2.2	Anlegget skal ha en fysisk områdesikring som effektivt hindrer inntrengning.
3.2.3	Anlegget skal ha god avstand til ikke-avsperrede områder.

5.1.9.2 Skallsikring - transformatorer

- 3.2.6 Alle hovedtransformatorer skal skallsikres fra alle kanter til over topp endemuffer ved hjelp av fjell eller transformatorceller av solid dobbeltarmert betong eller tilsvarende, og være konstruert og oppført etter anerkjente byggenormer. De skal herunder beskyttes og seksjoneres med høy brannmotstand etter fastsatt norm. De skal ha låsbare dører/porter eller fast montert gitter med høyt sikringsnivå etter fastsatt norm i alle mulige adkomster og lufteåpninger opptil minimum tre meter fra bakkeplan eller liknende.

5.1.9.2 Grunnsikring

Fysisk beskyttelse av transformatorer utføres som følger:

- Plasseres i fjellskjæring/-nisje, utstøpt skjæring/nisje i fast grunn eller i frittstående konstruksjon, eller i en kombinasjon av dette.
- Seksjoneres slik at hver transformator står i egen konstruksjon beskyttet på alle kanter.
- Beskyttes av konstruksjon med en utvendig høyde på minst 3 meter over terreng/toppen av eventuell tilfylling på alle kanter (også på bakside av eventuell skjæring).
- Transformator til og med topp endemuffer bør så langt mulig gis skjul og dekning i god avstand (flere hundre meter) sett fra omgivelsene. Dekning kan bestå av fjell (fast terreng) eller av konstruksjon.
- Konstruksjonen bør utføres med dekningstykkelse på minimum 200 millimeter plasstøpt dobbeltarmert betong. Betongkvalitet (fasthetsklasse) B 30 eller bedre. Armering tilsvarende sveiset nett nummer K 257 eller bedre.

Alternativt kan det for eksempel brukes:

- Prefabrikkerte betongelementer med netto betongtykkelse (dekningstykkelse) på minimum 200 millimeter, av god kvalitet montert i solid konstruksjon (avstivning, sammenføyning med videre).
- Ekvivalenter i stålelementer (dekningstykkelse minimum 20 millimeter, stålkvalitet bør oppfylle HB 200) eller ekvivalenter i aluminium kan vurderes. Ved dimensjonering skal det tas hensyn til ekstraordinære forhold og fysiske belastninger fra alle kanter.

Konstruksjon kun basert på murverk, hul- eller lettbetongblokker oppfyller ikke forskriftens krav.

Konstruksjonen bør minst tåle en belastning på 4 kN/m² eller mer fra alle kanter.

Alle monterte enheter som plater, rister, bjelker og lignende festes, eksempelvis med bolter fra innsiden, slik at de ikke kan fjernes fra utsiden.

Konstruksjonen bør utføres/utstyres som følger:

- Dører, porter osv sikres mot avløfting og med gode låseanordninger i sikkerhetsklasse 6 eller bedre etter EN, klasse 4 eller bedre etter FG.

- Solide dører/porter med en tykkelse som bør tilsvare 10 millimeter stål (KD/KP 10) eller ekvivalenter i aluminium.
- Stengsler med tilsvarende beskyttelse som cellevegg (betong, stål eller aluminium) monteres i transportåpning.
- Solid stål-/aluminiumsgitter i lufteåpninger, profil minimum 60 x 6 millimeter med senteravstand (c/c) ca. 80 millimeter + avstivninger eller tilsvarende.
- Alle føringer for kabler, rør, kanaler, kulverter, og andre mulige adkomster inn til transformatorcelle, muffehus og liknende sikres tilsvarende.
- Uten utvendige vinduer.
- Transformatorens lokale betjeningsorgan (for eksempel brytere og tappekran for olje) sikres.
- Vegger i konstruksjon, herunder seksjonerende vegger mellom flere transformatorer, utføres i minst brannklasse REI 120 M (M - hvor relevant), og seksjonerende dører med videre i brannklasse EI 120 eller bedre.
- Varmer, røyk, inntrengning med mer skal kunne oppdages straks og varsles.

For øvrig skal *FEF* og veiledningen til *FEF* § 4-9 Sikkerhetstiltak og sikkerhetsutstyr følges.

5.1.9.3 Skallsikring - øvrige anleggsdeler

3.2.4 Viktige anleggsdeler som driftsbygg, innendørs apparatanlegg, muffeanlegg og anlegg for stasjonsstrøm og styring, samt store og viktige komponenter med lang leveringstid, skal ha god skallsikring etter fastsatte normer for sikringsnivå.

De øvrige av stasjonens bygninger og liknende med viktige komponenter/ funksjoner bør utføres/ utstyres som følger:

- Alle utvendige dører/porter/adkomster i skallkonstruksjonen skal sikres mot avløfting og med låseanordninger av høy kvalitet, som bør oppfylle sikkerhetsklasse 5 etter EN og låser med mer i FG klasse 4 eller bedre.
- Alle føringer for kabler, rør, kanaler, kulverter, og andre mulige adkomster sikres tilsvarende.
- Innbruddshemmende vinduer klasse P7B eller bedre etter EN 356, i kontrollrom og liknende, og i andre rom som gir videre adgang til viktige deler av anlegget.
- Utføres uten vinduer i rom for kontrollutrustning (telerom og liknende) og nødstrøm.
- Yttervegger og seksjonerende vegger i brannklasse REI 60 M, dører med videre i EI 60 eller bedre.
- Varmer, røyk, inntrengning med mer skal kunne oppdages straks og varsles.

For SF₆ isolerte koblingsanlegg - se også eget punkt under.

5.1.9.4 Tilleggssikring

Ut fra analyse av anleggets betydning og lokale risiko og i henhold til egne akseptkriterier, skal ulike permanente forsterkninger av grunnsikringen vurderes og iverksettes. For transformatorceller, muffehus og liknende kan dette være ulike kombinasjoner av for eksempel:

- Økt betongtykkelse, betongkvalitet og/eller styrke på armeringen.
- Øke konstruksjonens evne til å tåle belastninger.
- Bjelkestengsler og dører/porters dimensjon/kvalitet økes i samsvar med ovennevnte.
- Gitter i luftåpninger forsterkes og/eller utføres som innstikkssikker – f.eks. som 75 x 75 x 10 millimeter vinkelstål med senter/senter avstand 50 mm + avstivninger.
- Utvendige dører/porter/adkomster i konstruksjon (skall) sikres låseanordninger av høyere kvalitet. Alternativt doble låseanordninger, hvorav én minst i høy sikkerhets-/ FG klasse.

For øvrige bygninger og liknende som har viktige komponenter/ funksjoner, gjøres tilsvarende oppgraderinger av sikringsnivået.

5.1.9.5 Sonesikring - innvendig av særlige viktige områder

3.2.5	Driftskontrollrom, datarom og andre rom for styring og samband skal være egne adgangskontrollerte soner, godt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.
-------	--

Sonesikring omfatter særlige viktige områder/ rom for lokalkontroll, samband, nødstrøm og lignende. Sikringsnivå tilpasses viktigheten av utstyret i sonen og nivået på den ytre skallsikringen, normalt minst FG-klasse 3 eller 4 og sikringsklasse 4 etter EN 1627.

5.1.10 Generelt om kraftstasjoner

Ved ombygging og liknende av eldre kraftstasjoner som ligger i dagen, kan det tas særlig hensyn til bevaring av deres arkitektoniske og historiske særpreg. Eldre stasjoner i dagen kan også ha en konstruksjon og beliggenhet som gjør det krevende å oppnå fullgod sikring. For slike kraftstasjoner må eier derfor gjennomgå anleggene og ut fra en vurdering i det enkelte tilfelle, så langt som mulig oppfylle beredskapsforskriftens krav etter prinsipper gitt i denne veiledningen.

5.1.11 Spesifikke krav til kraftstasjon klasse 1

Se bfe vedlegg 1 punkt 1.1.1 til 1.1.3:

5.1.11.1 Grunnsikring

Stasjonen og øvrige komponenter av betydning for drift og sikkerhet gis en ytre fysisk beskyttelse (skallsikring), minimum i form av låsbart fjellrom eller bygg som bør oppfylle sikkerhetsklasse 3 etter EN.

- Alle utvendige dører/porter/adkomster sikres med tilfredsstillende låseanordninger, sikkerhetsklasse (EN-norm) 3 og låser med videre i FG klasse 2 eller bedre.

- Hærverkshemmende vinduer i klasse P4A eller P5A etter EN, eller andre måter å beskytte vinduer og andre mulige adkomster på.
- Brannsikring etter veiledningen til FEF § 4-9 Sikkerhetstiltak og sikkerhetsutstyr, eller bedre.

5.1.11.2 Tilleggssikring

Områdesikring som gjerder/ porter og bommer og liknende vurderes i hvert enkelt tilfelle.

Ut fra analyse av anleggets betydning og lokal risiko skal man vurdere å gjennomføre ulike permanente forsterkninger av grunnsikringen. Dette kan være ulike elementer/ kombinasjoner av tiltak som gjelder for kraftstasjon klasse 2.

5.1.12 Spesifikke krav til kraftstasjon klasse 2

2.3	<i>For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
2.3.1	Kraftstasjoner i fjell skal ha en adgangskontrollert og fysisk sikret sone omfattende alle adkomster. Denne sonen skal oppfylle krav til godt sikringsnivå etter fastsatte normer for sikring. Herunder skal alle stasjoner ha minst én solid og låsbar stålport eller lignende i alle adkomster.
2.3.2	Kraftstasjoner i dagen skal ha god fysisk sikring med minimum et solid bygg med dører/porter, vinduer og øvrige adkomster etter fastsatte normer for sikringsnivå.
2.3.3	For kraftstasjoner i fjell og i dagen skal vitale komponenter som må plasseres utendørs, sikres etter samme krav som for transformatorstasjon, koblingsanlegg mv. i klasse 2.
2.3.4	Anleggets adkomster og vitale områder skal være utstyrt med effektive og pålitelige alarmer for brann, innbrudd, elektriske feil, og feil i styresystemer, samt ha etablert effektiv reaksjon for slike uønskede hendelser og handlinger.
2.3.5	Anlegget skal brannsikres og seksjoneres på hensiktsmessig måte med god brannmotstand etter fastsatt norm.
2.3.6	Driftskontrollrom, rom for styring og samband og lignende skal være egne og godt beskyttede adgangskontrollerte soner etter fastsatte normer for sikring og brannmotstand.

Kraftstasjon klasse 2 med vitale komponenter (se klasse 3) plasseres i beskyttende fjellrom. Dersom kraftverkstransformatorer og liknende plasseres i dagen bør disse seksjoneres og beskyttes som transformator klasse 2 med nødvendige lokale tillempninger.

Forutsatt at plasseringen i fjell gir solid beskyttelse, omfatter skallsikring mulige adkomster som drifts-, transport-, og andre adkomsttunneler, kabel- og ventilasjonssjakter samt andre åpninger som blant annet tverrslag og avløpstunneler.

5.1.12.1 Tilleggssikring

Områdesikring som gjerder/porter og bommer og liknende skal vurderes i hvert enkelt tilfelle. I henhold til egne akseptkriterier og ut fra lokal analyse av anleggets betydning og

risiko skal man vurdere å gjennomføre ulike permanente forsterkninger av grunnsikringen. Dette kan være elementer fra grunnsikring kraftstasjon klasse 3.

5.1.13 Spesifikke krav til kraftstasjon klasse 2 i fjell

For kraftstasjon i fjell skal det defineres en gjennomgående helhetlig sikringssone som omfatter alle mulige adkomster. Denne sikres med barrierer, som minimum bør oppfylle sikkerhetsklasse 4 etter EN og låser med videre etter FG klasse 3.

Adkomster eller liknende som kan lukkes permanent (eksempelvis tverrslag), bør støpes igjen med minimum 200 millimeter plasstøpt dobbeltarmert betong eller ekvivalenter i stål eller aluminium.

Konstruksjoner kun basert på murverk, hul-, lettbetongblokker eller liknende oppfyller ikke beredskapsforskriftens krav.

Vinduer i skallsikring skal minst utføres som innbruddshemmende, P6B etter EN 356 eller bedre.

Ytre komponenter/anleggsdeler sikres som for kraftstasjon klasse 2 i dagen.

5.1.14 Spesifikke krav til kraftstasjon klasse 2 i dagen

Kraftstasjoner i dagen med alle ytre komponenter/inn ganger av betydning for drift og sikkerhet, skal sikres med solide bygg og beskyttende konstruksjoner. Mulige adkomster sikres med luker, rister eller liknende som minst oppfyller sikkerhetsklasse 3 etter EN. Tilsvarende sikres bruksinn ganger med dører, porter og liknende som minst oppfyller sikkerhetsklasse 3 etter EN og utstyres med låser etter FG klasse 2 eller bedre. Vinduer skal være hærverkshemmende (P5A) eller fortrinnsvis innbruddshemmende, (P6B) etter EN 356.

5.1.14.1 Sonesikring - innvendig av særlige viktige områder

Sonesikring omfatter særlige viktige områder/rom for lokalkontroll, samband, nødstrøm og lignende. Sikringsnivå tilpasses viktigheten av utstyret i sonen og nivået på ytre skallsikring, normalt minst FG-klasse 3, eller sikringsklasse 3 eller 4 etter EN 1627.

5.1.15 Spesifikke krav til kraftstasjon klasse 3

3.3	<i>For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:</i>
3.3.1	Alle vitale komponenter skal legges i beskyttende fjellrom og det skal etableres en omsluttende adgangskontrollert og fysisk sikret sone som omfatter alle mulige adkomster med høyt sikringsnivå etter fastsatt norm. Herunder skal alle stasjoner ha minst én solid og låsbar stålport eller lignende i alle adkomster. Vitale komponenter som må legges i dagen, sikres som for transformatorstasjon, koblingsanlegg mv. i klasse 3.
3.3.2	Anlegget skal seksjoneres på en hensiktsmessig måte med brannsikring som gir høy brannmotstand etter fastsatte normer og relevante forskrifter.
3.3.3	Skal ha utstyr og prosedyrer for effektiv deteksjon, alarmer, verifikasjon og reaksjon mht. uønskede hendelser og handlinger. Som et minimum skal dette omfatte adkomster og stasjonens vitale områder.

3.3.4	Driftskontrollrom, rom for styring og samband og lignende skal være egne adgangskontrollerte godt beskyttede soner etter fastsatte normer for hhv. fysisk sikring og brannmotstand.
-------	---

Kraftstasjon i klasse 3 skal plasseres i beskyttende fjellrom. Dette gjelder alle deler av kraftstasjonen som ivaretar vitale funksjoner fra og med tilløpstunnel, trykksjakt med ventil/lukekammer, turbin, generator - til og med henholdsvis kraftverkstransformator og avløpstunnel, samt rom for styresystemer, samband og intern strømforsyning. Der kraftstasjon helt eller delvis må plasseres i dagen, se krav til sikring for kraftstasjon i dagen.

Forutsatt at plasseringen i fjell gir solid beskyttelse, omfatter skallsikring mulige adkomster som drifts-, transport-, og andre adkomsttunneler, kabel-, ventilasjonsjakter og andre åpninger, samt tverrslag og avløpstunneler.

5.1.15.1 Fysisk utførelse

For alle adkomster skal det defineres en gjennomgående helhetlig sikringssone. Denne sikres med solide barrierer, som minimum bør omfatte én eller flere kombinasjoner av følgende alternativer:

- Heldekkende (vegg til vegg, gulv til tak) stålgitter, for adkomster kommer i tillegg solid innfestet stålpport eller ståldør.
- Solid stålgitter med profil tilsvarende min. 60 x 6 millimeter med senteravstand ca. 80 millimeter + avstivninger.
- Solide dører/porter med tykkelse tilsvarende 10 mm stål (KD/KP 10) eller tilsvarende.
- Dører/porter skal sikres mot avløfting og med låseanordninger av høy kvalitet som bør oppfylle sikkerhetsklasse 5 etter EN og låser med videre etter FG klasse 4 eller bedre. Tofløyede porter skal sikres med midtsikring oppe og nede av tilsvarende kvalitet.
- Adkomster eller liknende (eksempelvis transportganger) som bare unntaksvis skal kunne åpnes, kan alternativt sikres med heldekkende armert betongvegg med bjelkestengsel i transportåpning eller tilsvarende i stål eller aluminium.
- Betongtykkelse i vegger og bjelkestengsler skal være minimum 200 millimeter. Betongkvalitet minimum B 30. Armering vegg tilsvarende sveiset nett K 189 eller bedre, ekvivalent armering for bjelkestengsel.
- Adkomster eller liknende som kan lukkes permanent (for eksempel tverrslag), bør støpes igjen med minimum 200 millimeter plaststøpt dobbeltarmert betong. Betongkvalitet B 30 eller bedre. Armering tilsvarende sveiset nett K 189 eller bedre. I tverrslag må selve stengslet mot vanntrykk dimensjoneres for dette.

Istedenfor 200 millimeter betong kan ekvivalenter i 20 millimeter stålplater benyttes. Ekvivalenter i aluminium kan vurderes. Stål og aluminium må være av god kvalitet siden legering med videre er helt avgjørende for hardhet og strekkfasthet. Stål eller aluminiumsplater/-bjelker må festes (boltes fra innsiden eller liknende) slik at disse ikke kan fjernes eller løftes ut av feste/føringer fra utsiden.

Alle barrierer bør som et minimum tåle sideveis (horisontalt) belastning på 2 kN/m² eller mer.

Konstruksjon kun basert på murverk, hul- eller lettbetongblokker eller liknende oppfyller ikke beredskapsforskriftens krav.

Utføres uten vinduer i skallsikring – jf sikringssone.

For alle adkomster beregnet for hyppig/daglig, bruk bør det i tillegg til ovennevnte være en ytre sikring/barriere i form av låsbare rulleporter eller gangdører i sikkerhetsklasse 2 eller 3 etter EN, samt eventuelt ytre luker, rister med videre av tilsvarende kvalitet. Slike ytre innganger skal sikres med tilfredsstillende låseanordninger, sikkerhetsklasse 3 etter EN og låser med videre etter FG klasse 2 eller bedre.

Finnes ikke slik ytre sikring, bør sikkerhetsklassen (EN/FG) heves i skallsikringens adkomster.

Andre komponenter skal sikres som følger:

- Vitale utendørs komponenter som inntaksluker, andre tappeanordninger, tverrslag og vannvei og avløp for kraftstasjonens drift og sikkerhet sikres med betonghus, gitter, ståldører og låser etter krav som for tilsvarende barrierer i skallsikring.
- Kraftverkstransformatorer, fortrinnsvis én per generator, plasseres innvendig i fjellhall adskilt fra generator-/turbinhall og øvrig adkomst. De skal seksjoneres fra hverandre og øvrig stasjon med vegger/bjelkestengsler og dører som minimum bør ha brannklasse REI 120 (M – hvor dette relevant). Se også krav til brannsikkerhet.
- Rom for kontroll, styring, samband, nødstrøm og likende skal sikres med vegger og låsbare dører som minimum bør ha brannklasse REI 60 (M) og EI 60. Se også krav til brannsikkerhet.

For øvrig forutsettes det at brannsikringen er utført etter veiledningen til *FEF* § 4-9 Sikkerhetstiltak og sikkerhetsutstyr.

5.1.15.2 Tilleggssikring

Ut fra lokal analyse av anleggets betydning og risiko vurderes og iverksettes ulike permanente forsterkninger av grunnsikringen. Særlig for steder som ikke kan overvåkes eller for særlig eksponerte anlegg eller komponenter, er dette relevant. Dette kan være ulike kombinasjoner av for eksempel:

- Dører/ porter/ gitter og andre stengsler forsterkes eller dubleres og sikres med låseanordninger av høyere kvalitet/ sikkerhetsklasse.
- Øvrige konstruksjonsdelers evne til å tåle ulike belastninger og inntrengningsforsøk økes.

5.1.15.3 Sonesikring - innvendig av særlige viktige områder

Sonesikring omfatter særlig viktige områder/ rom for lokalkontroll, samband, nødstrøm og liknende. Sikringsnivået skal tilpasses viktigheten av utstyret i sonen og nivået på den ytre skallsikringen, normalt minst FG-klasse 3 eller 4 og sikringsklasse 4 etter EN 1627.

5.1.16 Driftssentraler med tilhørende bygg – alle klasser

Veiledningen tar utgangspunkt i at driftskontrollsystemet er bygget redundant etter metode 2, dublering i samme bygg (jf veiledning til kapittel 7). Dersom man velger andre løsninger til redundans – for eksempel metode 1 (alternativt sted) kan kravene til skallsikring og liknende reduseres noe. For eksempel i et redundant driftskontrollsystem i klasse 3 hvor det alternative stedet for driftskontroll er plassert et helt annet sted, kan det aksepteres at dette alternative stedet fysisk sikres (beskyttes) etter krav for klasse 2.

Selv om driftssentralssystemet bygges redundant og funksjon kan ivaretas fra et annet sted, skal operatørrom og liknende sikres mot inntrengning, hærverk, urettmessig overtakelse og hindre lokal tilgang til IKT systemene. Det skal være nødstrøm etter klasse 3 på minst ett sted i tilfelle strømutfall over et større område.

Brann i eller nær driftskontrollsystemet må oppdages så fort som mulig, slik at slukkearbeidet kan starte tidligst mulig og konsekvensene begrenses. Enheter med driftssentraler (gjelder alle klasser) bør derfor installere automatisk brannalarmanlegg med detektorer i alle rom i den delen av bygget hvor driftssentralen med tilbehør er plassert. Det kan også gjelde rom som ligger over eller under driftssentralen og/eller tilhørende rom dersom etasjeskillene ikke tilfredsstiller REI 120 M brannmotstand, bygget ikke er fullsprinklet, eller på annen måte har tilsvarende sikring mot spredning av røyk og brann.

Krav til branncelle for driftssentraler etter denne forskriften er primært for å hindre brannspredning inn til driftsentralens rom og funksjoner eller mellom driftssentralens redundante systemer (rom).

Brannsikringen generelt skal blant annet omfatte:

- Et deteksjonssystem med tilstrekkelig antall og riktig plasserte detektorer, sammenkoblet i et system, fortrinnsvis med forskjellige egenskaper (ioniske, optiske og varmesensitive).
- Et system for effektivt og hurtig mottak, reaksjon (alarm) og videre varsling av eventuell deteksjon.
- Nødvendig slukkeutstyr av hensiktsmessig type, antall og plassering.
- Brannalarmen skal døgntilgjengelig varsle driftspersonell, enten stedlig personell eller hjemmevakt, eller en annen betjent drifts- eller vaktsentral.
- Brannvarsling bør også gå til lokal brann- og redningsetat.

Teksten under forklarer nærmere kravene som gjelder for de ulike klassene.

5.1.17 Spesifikke krav til driftssentraler klasse 1

1.2.1 Driftssentraler

1.2.1.1 Driftssentraler skal plasseres i et bygg med normal brann- og innbruddssikkerhet.

1.2.1.2 Skal ha et effektivt innbrudds- og brannvarslingssystem.

1.2.1.3 Skal være normalt fysisk sikret etter fastsatt norm.

Driftssentralen gis følgende fysiske beskyttelse:

- Skal plasseres i et bygg med minimum normal brann- og innbruddssikkerhet.
- Utføres som branncelle(r) med en brannmotstand på minst EI 30 (selvlukkende dører vurderes). Tilsvarende brannsikring for kabelgjennomføringer med mer.
- Utstyres med solide låsbare dører som sammen med annen sikring av adkomster bør oppfylle sikkerhetsklasse 3 (enkel innbruddsikring) etter EN.
- Operatørrom bør ha hærverkshemmende vinduer etter EN 356. For øvrige (tekniske) rom unngås vinduer.
- Bør ha brann- og innbruddsalarm med effektiv varsling av hjemmevakt, lokalt brannvesen eller annen bemannet driftssentral, installert for driftssentralen. Branncelle(r) med tilstøtende rom, også over og under.
- Nødvendige slukkemidler for å slå ned en mindre brann raskt, må være tilgjengelig.

5.1.18 Driftssentraler klasse 2 og 3

Dersom operatørrom er plassert høyere oppe i bygget og driftskontrollfunksjonene kan betjenes fra for eksempel et sikret beredskapsrom i tilknytning til prosessmaskinene med videre plassert lengre ned i bygget, kan de bygningstekniske kravene til operatørrommet/området (vegger, gulv, tak) hvor den bygningstekniske konstruksjon for øvrig gjør dette hensiktsmessig, reduseres til den innbruddsikring som generelt er angitt for vedkommende klasse.

5.1.19 Spesifikke krav til driftssentraler klasse 2

2.4.1 *Driftssentraler*

- 2.4.1.1 Driftssentraler skal plasseres i et bygg med god brann- og innbruddssikkerhet.
- 2.4.1.2 Skal være en egen fysisk sikret adgangskontrollert sone og utføres som egen branncelle med god brannsikkerhet og brannmotstand etter fastsatt norm.
- 2.4.1.4 Operatørrom og andre bygningsdeler av vesentlig betydning for driftskontrollfunksjonene skal være normalt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.

Driftssentralen gis følgende fysiske utførelse:

- Utføres som egen branncelle(r) med en brannmotstand på minst EI 60 (REI 60 M – hvor relevant). Kabelgjennomføringer med mer skal sikres tilsvarende. Det samme gjelder for vegger, kabelføringer med mer, mellom de redundante delene av anlegget. Det bør installeres selvlukkende dører. Tilsvarende brannsikring av kabelgjennomføringer med mer.
- For rom og bygningsdeler av vesentlig betydning for driftskontrollfunksjonene, det vil si hvor det er plassert viktig utstyr (datarom/ prosessmaskiner, sambandsrom/ terminalutstyr og liknende), samt øvrige relevante rom (operatørrom, strømforsyning/ batterirom og liknende), utføres gulv, tak og utvendige vegger i

minimum etter kravene i EN 1992 (tidligere NS 3473 - *Prosjektering av betongkonstruksjoner - Beregnings- og konstruksjonsregler*). Er ikke dette mulig skal slike vegger vurderes forsterket med for eksempel stålplater eller solid kryssfiner. Ventilasjonsåpninger og liknende sikres med gitter eller stålplater.

- Dører, låser, gitter med videre i utvendige vegger, bør utføres som sikkerhetsklasse 4 (minimum 3) etter EN (1627 med videre). Indre sonesikring utføres som sikkerhetsklasse 3 eller 4. Andre dører minimum EI 60, og utført i stål dersom de også skal tjene som sikring mot inntrengning. Selvlukking vurderes.
- Operatørrom utstyres med sikkerhetsglass som minimum oppfyller klasse P6B ("innbruddshemmende" glass) etter EN 356. Slikt glass vil også være FG-godkjent. Vindusflatenes areal vurderes. For rom som ikke er fast arbeidsplass, kan et alternativ være å utstyre slike vinduer med solide stållemmer/ skodder eller liknende som enkelt kan trekkes for og låses. Rom for prosessanlegg, front-end, telerom og liknende, bygges uten vinduer.
- Brann- og innbruddsalarm med effektiv varsling skal installeres i hele driftssentralen (branncelle(r)) med tilstøtende rom. Brannalarmen skal døgntkontinuerlig varsle driftspersonell, enten stedlig personell eller hjemmevakt, lokalt brannvesen eller annen bemannet driftssentral.
- Slukkemidler for raskt å slå ned en mindre brann må være tilgjengelig. Automatisk slukkeanlegg bør vurderes.

5.1.20 Spesifikke krav til driftssentraler klasse 3

3.4.1	<i>Driftssentraler</i>
3.4.1.1	Driftssentraler skal plasseres i et solid bygg med god brann- og innbruddssikkerhet.
3.4.1.2	Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger.
3.4.1.3	Skal være egen fysisk sikret adgangskontrollerte sone(r) og utføres som egen branncelle(r) med høy brannsikkerhet og brannmotstand etter fastsatte normer.
3.4.1.4	Operatørrom og andre bygningsdeler av vesentlig betydning for driftskontrollfunksjonene skal være godt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.

Driftssentralen gis følgende fysiske utførelse:

- Plasseres i et solid bygg med meget god brann og innbruddssikkerhet.
- Utføres som egen branncelle(r) med en brannmotstand på minst EI 60 og REI 60 M for bygningsdeler hvor dette er relevant. Motstandstiden skal økes til 120 minutter dersom det ikke er installert automatisk slukkeutstyr. Ved dokumentert nærhet til permanent bemannet brannutrykningsenhet kan sistnevnte krav reduseres, men ikke til mindre enn EI 60/ REI 60 M, da dette også skal tjene som skallsikring. Selvlukkende dører minimum EI 60 C. Tilsvarende brannsikring av

kabelgjennomføringer med mer. Samme gjelder for vegger, kabelføringer med mer mellom de redundante delene av anlegget.

- Operatørrom utstyres med sikkerhetsglass som minimum oppfyller klasse P7B (P8B vurderes) ("innbruddshemmende" glass) etter EN 356. Slikt glass vil også være FG- godkjent. Vindusflatenes areal må vurderes. For rom som ikke er fast arbeidsplass, kan et alternativ være å utstyre slike vinduer med solide stållemmer/skodder eller liknende som enkelt kan trekkes for og låses. Rom for prosessanlegg, front-end, telerom og liknende bygges uten vinduer.
- For rom/bygningsdel av vesentlig betydning for driftskontrollfunksjonene, hvor det er plassert viktig utstyr (datarom/ prosessmaskiner, sambandsrom/ terminalutstyr og likende), samt øvrige relevante rom (operatørrom, strømforsyning/ batterirom og liknende) bør gulv, tak og utvendige vegger utføres i minimum 200 millimeter dobbeltarmert betong. Dimensjonene kan reduseres til minimumskravene i EN 1992 (tidligere NS 3473 - *Prosjektering av betongkonstruksjoner - Beregnings- og konstruksjonsregler*). Er ikke dette mulig skal slike vegger med videre forsterkes med for eksempel 3 til 4 mm stålplater eller liknende med solid innfesting. Ventilasjonsåpninger og liknende sikres med gitter eller stålplater.
- Dører, låser, gitter med videre i utvendige vegger, bør utføres som sikkerhetsklasse 5 (minimum 4) etter EN (1627 med videre). På utsatte steder bør KD 10 eller tilsvarende vurderes. Indre sonesikring utføres som sikkerhetsklasse 4. Andre dører minimum EI 60, og utført i stål dersom de også skal tjene som sikring mot inntrengning. Selvlukking vurderes.
- Brann og innbruddsalarm med automatisk brannalarmanlegg med detektorer i alle rom i den delen av bygget hvor driftssentralen med tilbehør er plassert. Dette gjelder både i og utenfor driftssentralens branncelle(r), samt i etasjen over og under, oppganger, ventilasjonsjakter med mer. Dette må sees forhold til de ulike veggens og etasjeskilleres brannmotstand, og byggets brannsikkerhet for øvrig.
- Brannalarmen skal døgntkontinuerlig varsle driftspersonell, enten stedlig personell, hjemmevakt, lokalt brannvesen eller annen bemannet driftssentral. Enheten må sørge for tilstrekkelig antall detektorer, sammenkoblet i et system, med forskjellige egenskaper (ioniske, optiske og varmesensitive). Om mulig bør brannvarsling også gå til lokal brann- og redningsetat.
- Slukkemidler for raskt å slå ned en mindre brann må være tilgjengelig. Installering av automatisk slukkeutstyr skal vurderes.

5.1.21 Spesifikke krav til sambandsanlegg klasse 1

1.2.2 For sambandsanlegg gjelder følgende krav:

- 1.2.2.1 Sambandsanlegg regnes normalt som en del av det driftskontrollsystem de betjener og skal planlegges og utføres etter de påregnelige påkjenninger de kan bli utsatt for.
- 1.2.2.2 Anlegget skal sikres mot uønskede hendelser og handlinger som innbrudd, hærverk, sabotasje og brann.

5.1.22 Spesifikke krav til sambandsanlegg klasse 2

2.4.2 *Sambandsanlegg:*

- 2.4.2.1 Sambandsanlegg regnes normalt som en del av det driftskontrollsystem de inngår i.
- 2.4.2.2 Anlegget skal planlegges og utføres slik at de tåler de maksimale påkjenninger de kan bli utsatt for.
- 2.4.2.3 Anlegget skal sikres mot uønskede hendelser og handlinger som innbrudd, hæververk, sabotasje og brann.

5.1.23 Spesifikke krav til sambandsanlegg klasse 3

3.4.2 *Sambandsanlegg:*

- 3.4.2.1 Anlegget skal utføres så fysisk, elektrisk og elektronisk robust at det tåler påregnelig uvær og andre ytre påkjenninger, herunder atmosfæriske og elektromagnetiske forstyrrelser
- 3.4.2.2 Utsatte anleggsdeler som kabler, master og antenner/ radiospeil skal utføres særlig robuste, og bygg med adkomster som dører og vinduer må gis god sikring etter fastsatte normer for fysisk sikring.

Sambandsanlegg skal planlegges og utføres etter de maksimalbelastningene (uvær, ising med videre) de kan bli utsatt for. Dette gjelder særlig utsatte komponenter med tilhørende oppheng/føringer og festeanordninger som kabler, master, antenner, radiospeil, HF-sperrer med mer.

Sambandsanlegg skal gis en tilfredsstillende fysisk sikring etter klasse og risiko for inntrenging, sabotasje, brann og andre former for ødeleggelse. Dette kan gjøres eksempelvis ved bruk av ikke brennbare materialer, brannslukningsanlegg/-utstyr, brann- og innbruddsalarm. Vinduer skal unngås i alle anlegg, eventuelt skal de sikres med hæververks- eller innbruddshemmende glass, stållemmer, solide gitter eller liknende som låses eller boltes fra innsiden.

Antenneanlegg, master og kabelføringer sikres mot hæververk, sabotasje, uønsket adgang og brann. Dette omfatter tiltak som bruk av ikke brennbare materialer, beskyttelse av kabler, inngjerding av master og tildekking/beskyttelse av kabeltrasé fram til disse.

Strømforsyning og samband bør føres inn i anlegget gjennom jordkabler eller gis annen beskyttelse. Master beskyttes med klatrehindre.

Viktige eller utsatte sambandsanlegg i klasse 2 og 3 skal vurderes utført med relevante sikringstiltak som for driftssentral i samme klasse, slik at driftskontrollsystemet gis en helhetlig og balansert beskyttelse etter de ulike elementers betydning. I klasse 3 bør utvendige vegger i så fall bygges i 200 millimeter dobbeltarmert betong. Dimensjonene kan reduseres til minimumskravene i NS 3473 for vegger mellom rommene. Dører i utvendige vegger KD 10. Andre dører EI 60 (stål) eller bedre.

Sambandsanlegg i klasse 2 og mindre utsatte anlegg i klasse 3 gis solid utførelse ved plassering i bygg av eksempelvis betongelementer, stålcontainer, samt ståldører. Rene trebygninger og liknende bør unngås.

5.1.24 Nærmere om gassisolerte koblingsanlegg og liknende

Gassisolerte (helkapslede) koblingsanlegg og tilsvarende vitale og relativt sårbare anleggsdeler i alle energianlegg i klasse 2 og 3 plasseres i avlukket/sikret fjellrom eller betongbygg. Betongbygg utføres etter vanlig god byggestandard med vegger, golv og tak i minimum 20 centimeter dobbeltarmert betong. Apparatsal, rom for styresystemer og liknende utføres uten vinduer. Øvrige vinduer utføres som innbruddshemmende etter EN 356 og adkomster med videre sikres.

Sikringstiltak og sikringsnivå utføres for øvrig som for respektive klasse og anleggstype.

5.1.25 Nærmere om sikringstiltak ved vedlikehold, reparasjoner o.l.

Alle nødvendige sikringstiltak, for anlegg i alle klasser, bør være ferdig montert og sikret mot at de kan fjernes av uvedkommende. Bare ved arbeid på stedet, kan beskyttelsestiltak helt eller delvis fjernes av praktiske grunner og av hensyn til arbeidssikkerheten. I slike situasjoner forutsetter vi at det på forhånd gjøres grundige risikovurderinger og kompenserende tiltak. Dersom skallsikringen må svekkes under arbeidet, må det vurderes å styrke områdesikringen, og omvendt. Er det ikke mulig å oppnå tilstrekkelig sikringsnivå på denne måten, må vakthold etableres. Anleggene skal være sikret når arbeidsstedet forlates for dagen. Se for øvrig veiledning til § 5-1 om adgangskontroll ved bygge- og installasjonsarbeider.

Generelt skal adkomster være låst når det ikke er personell til stede. Sikringstiltak må ikke være til hinder for tilfredsstillende rømningsveier når personell er til stede.

Arbeid som medfører at det må tas hull i brannskiller eller fjerning av branntetting, må vies særlig oppmerksomhet. Permanent eller midlertidig branntetting må etableres før arbeidsstedet forlates for dagen.

Dersom arbeidet pågår over flere dager, må det være et godt system for kontroll med at alle typer sikringstiltak så langt mulig virker når arbeidsstedet forlates.

Dersom adgangskontrollen må deaktiveres eller det må gjøres endringer på sensorer, kabler, kameraer og liknende, må man likedan forsikre seg om at funksjonaliteten er gjenopprettet før annen sikring eller vakthold oppheves. For nærmere veiledning om adgangskontroll, se § 5-1 Sikringsplikt.

5.1.26 Nærmere om fysisk beskyttelse av eksisterende anlegg

Som hovedregel krever vi ikke at det skal utføres sikringstiltak som medfører større ombygginger av eksisterende anlegg. Unntak kan gjøres for særlig viktige eller særlig dårlig sikrede anlegg. Dette innebærer at det normalt ikke blir stilt krav om å gjennomføre tiltak som innebærer større eller uforholdmessig kostbare endringer i planløsninger, bygningsmasse eller i arrangementen av de elektriske høyspenningsanleggene.

Dersom det er vedtatt eller foreligger konkrete planer om at anlegget skal bygges om eller utvides i relativt nær framtid (< 10 år), kan det vurderes om relevante sikringstiltak for de delene som skal bygges om, inntil videre utstår og heller tas med i denne ombyggingen. Dette gjelder bare for relativt kostbare tiltak eller når tiltak på et eldre anlegg ikke synes å

være hensiktsmessig. Nevnte vurdering og planer må i så fall kunne dokumenteres og annen kompenserende beredskap forberedes.

Eldre kraftforsyningsanlegg i dagen kan være anlegg med arkitektoniske og historiske særpreg. Noen er fredet eller har fått status som kulturminne. Andre kan ha en konstruksjon og beliggenhet som gjør fullgod sikring utfordrende. For disse skal sikringstiltak tilpasses så langt mulig etter stedlige forhold og nevnte hensyn.

For de bestemmelsene hvor anleggets art og alder ikke har vesentlig betydning for gjennomføringen av tiltaket, gjelder bestemmelsene som for nye anlegg.

5.1.26.1 Områdesikring - alle klasser

a. Gjerder, porter med videre som i konstruksjon og plassering tilfredsstiller kravene i § 4-5 Installasjoner i veiledning til *FEF* eller tidligere retningslinjer for sikring av kraftforsyningsanlegg (RSK), kreves ikke ombygd, men må holdes i forsvarlig stand og forsterkes der det er åpenbare mangler eller svakheter.

b. Tilleggssikring (ekstra gjerder, veibommer o.l.) vurderes i det enkelte tilfellet.

5.1.26.2 Skallsikring

Klasse 1

Anleggets bygningsmasse og eventuelle andre beskyttende tiltak skal gjennomgå, og åpenbare mangler eller svakheter rettes.

Klasse 2

I tillegg til ovennevnte for klasse 1 gjelder følgende:

a. Alle dører og liknende - utvendig eller innvendig – som er eller bør være en del av de fysiske sikringstiltakene, må minst fylle kravene til ståldør A 60 etter tidligere standard. Tilsvarende må alle vinduer som er eller bør være en del av skallsikringen rundt vitale deler av anlegget, som et minimum være utført som hærverkshemmende ved glass, gitter eller liknende. Øvrige mulige atkomster (kabelsjakter, luftekanaler o.l.) sikres tilsvarende. Der nye tiltak må utføres for å fylle disse kravene, bør disse så langt mulig utføres etter denne forskrift. For eldre kraftstasjoner i dagen som i sin tid ble utført med mange eller store vindusflater, kan det gjøres unntak, men kompenserende tiltak som alarmer eller liknende må da vurderes.

b. Hovedtransformatorer i klasse 2-anlegg bør skallsikres. Der dette ikke er gjort i det hele tatt, må dette utføres etter denne forskrift ved neste ombygging eller utvidelse av anlegget. Der det delvis er utført, må tiltaket fullføres ved at for eksempel transport-, inspeksjons- og lufteåpninger så langt mulig sikres med porter, gitter etter denne forskrift.

c. Kraftstasjoner i klasse 2 i fjell sikres med minst en solid og låsbar port, gitter eller liknende i alle atkomster som fører inn til stasjonens vitale deler. Der nye tiltak må utføres for å fylle disse kravene, bør disse så langt mulig utføres etter denne forskrift.

Klasse 3

I tillegg til ovennevnte for klasse 2 gjelder følgende:

a. Alle vinduer som er eller bør være en del av skallsikringen, må som et minimum være utført som innbruddshemmende ved glass, gitter eller liknende. Øvrige mulige atkomster som dører, kabelsjakter, luftekanaler og liknende sikres tilsvarende. Kontrollrom med videre og gassisolerte koblingsanlegg må vies særlig oppmerksomhet.

b. Alle krafttransformatorer i klasse 3 kraftforsyningsanlegg skallsikres, så langt som praktisk mulig. Der skallsikring og ulike former for beskyttelse i noen grad er utført, kan det bygges videre på dette. Transport-, inspeksjons- og lufteåpninger skal sikres med porter, gitter med videre etter denne forskrift.

c. I tillegg til dagporten(e) skal som hovedregel alle kraftstasjoner i klasse 3 (i fjell), ha minst én solid og låsbar stålport (kraftverksport eller liknende) i (hver av) adkomst-tunnelen(e). Alle øvrige adkomster inn til kraftstasjonen som transporttunnel, kabelsjakter, luftekanaler o.l. som fører inn til stasjonens vitale deler (herunder også lukehus o.l.) sikres med porter, gitter og lignende med tilsvarende sikringsnivå. Der nye tiltak må utføres for å fylle disse kravene, skal disse så langt som mulig utføres etter denne forskrift.

5.I.27 Låsanordninger – alle klasser

For å oppfylle forskriftens krav, må alle låser med beslag og innfesting på stengsler som inngår i område- og skallsikringen være FG-godkjent eller tilsvarende. I områdesikringen bør det minst brukes FG klasse 2 og for skallsikringen FG klasse 3. Hvis låsene for å oppfylle dette kravet likevel må skiftes ut, brukes FG/ sikkerhetsklasse for vedkommende anlegg og klasse etter denne forskrift.

Del II Uønskede hendelser og handlinger skal oppdages

5.II.1 Kraftforsyningsanlegg i klasse 1

Det er normalt tilstrekkelig med et regelmessig tilsyn og etablerte rutiner for å håndtere hendelser og unormale tilstander.

Systemer for å oppdage eller eventuelt å utløse alarm ved eksempelvis innbrudd, brann og teknisk svikt, anbefales. Der lokale risikoforhold tilsier det, forutsettes det at slike alarmsystemer etableres. Ved utsatte anlegg bør alarmer vurderes som for klasse 2.

Samme vurdering skal også gjøres for administrasjonsbygg, lager med videre av betydning for ledelse og drift, beredskap og sikkerhet.

5.II.2 Kraftforsyningsanlegg i klasse 2

2.1. For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:

2.1.1 a. Uønskede hendelser og handlinger skal oppdages raskt og håndteres av et effektivt reaksjonsmønster.

2.2. For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:

- | | |
|-------|---|
| 2.2.1 | Anlegget skal være utstyrt med effektive og pålitelige alarmer for brann, innbrudd, elektriske feil og feil i styresystemer, samt ha etablert tiltak for effektiv reaksjon. |
|-------|---|

2.4	<i>For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
------------	---

2.4.1	<i>Driftssentraler</i>
--------------	-------------------------------

- | | |
|---------|--|
| 2.4.1.1 | Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, varsling og rask reaksjon ved uønskede hendelser og handlinger. |
|---------|--|

For alle kraftforsyningsanlegg i klasse 2 skal det være etablert tiltak for raskt å oppdage og kunne håndtere uønskede hendelser og handlinger på en effektiv måte.

Vi forutsetter at anlegget via driftskontrollsystem eller på annen måte har systemer som løpende overvåker anleggets tekniske tilstand og drift, alarmerer om feiltilstander, og har prosedyrer for nødvendig inngripen og feilretting.

I tillegg til regelmessig tilsyn og gode rutiner, skal det som et minimum være installert innbrudds- og brannalarm (oppdagelse og varsling) i alle viktige deler av anlegget. Alarmene skal raskt og effektivt varsle videre til vaktentral, driftssentral eller annen vaktordning med personell som er kompetent til å følge opp den uønskede situasjonen.

Se også Del I Fysisk utførelse – beskyttelse om brannsikring.

Det skal være beredskap for raskt å kunne sende ut folk for stedlig observasjon, verifikasjon av hendelsen og gjennomføre de tiltakene som situasjonen krever. Det må i tillegg være gjennomførbare planer for skjerpet tilsyn og kontroll med anlegg i ekstraordinære situasjoner. Det skal legges til rette for varsling av og samarbeid med forsvaret, politi og andre nødetater.

Det skal til enhver tid holdes kontroll på hvem som har rettmessig adgang til anlegget, i henhold til § 5-1 Adgangskontroll.

5.II.3 Kraftforsyningsanlegg i klasse 3

3.1	<i>For transformatorstasjoner, koblingsanlegg/-stasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:</i>
------------	--

- | | |
|----------|--|
| 3.1.1 a. | Alle uønskede hendelser og handlinger skal oppdages straks, kunne verifiseres og håndteres av et effektivt reaksjonsmønster. |
|----------|--|

3.2.	<i>For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i over nevnte punkt 3.1:</i>
-------------	--

- | | |
|-------|---|
| 3.2.1 | Anlegget skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmering, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger. |
|-------|---|

3.3	<i>For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:</i>
3.3.3	Skal ha utstyr og prosedyrer for effektiv deteksjon, alarmer, verifikasjon og reaksjon mht. uønskede hendelser og handlinger. Som et minimum skal dette omfatte adkomster og stasjonens vitale områder.

3.4	<i>For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 3.1:</i>
3.4.1	<i>Driftssentraler</i>
3.4.1.2	Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger.

I tillegg til krav for klasse 2 etter forrige punkt gjelder følgende:

Alle kraftforsyningsanlegg i klasse 3 skal utstyres med mekanismer (elektroniske, optiske eller mekaniske systemer, vakthold eller annet) for straks å oppdage og reagere på uønskede hendelser og handlinger, og på den måten bidra til å forebygge og hindre dem. Dersom slike hendelser likevel inntreffer, skal det være mulig å verifisere og dokumentere dem i ettertid.

Disse mekanismene skal som et minimum oppfylle følgende krav:

Oppdage og varsle (alarm) all uønsket ferdsel, innbruddsforsøk og liknende handlinger innenfor et klart og for det enkelte anlegg logisk definert område. Dette skal som et minimum omfatte anleggets vitale komponenter med tilhørende skallsikring (bl.a. hovedtransformatorer, innendørs koblingsanlegg, driftsbygg med kontrollrom, prosessmaskiner, samband, nødstrømsforsyning med videre) se også § 5-1 Adgangskontroll, eventuelt (alternativt) alle adkomster for den delen av anlegget som ligger i fjell.

Det skal ikke være mulig å trenge seg inn i et anleggs definerte skallsikring og sikkerhetssoner uten at dette oppdages og varsles.

Tilsvarende alarmsystem etableres for å kunne oppdage og varsle brann, branntilløp, røykutvikling og liknende. Systemer for oppdagelse og varsling av andre typer uønskede hendelser (for eksempel gasslekkasjer, oversvømmelse, varmgang, elektriske eller mekaniske feil) skal vurderes for de enkelte anlegg.

Når alarmen utløses eller for andre relevante situasjoner, skal det i tillegg være et system (styrbare eller faste kameraer, TV skjermer, PC eller liknede) for å kunne føre løpende oversikt, oppdagelse og verifikasjon ("overvåkning") av alle vesentlige deler av anlegget, eventuelt adkomster til fjellanlegg. Dette skal straks kunne oppdage og så langt mulig gi en oversikt over hva som skjer eller kan ha skjedd.

Det må være et opptaks- og lagringssystem for bilder, videoer og liknende, slik at hendelsene kan verifiseres og dokumenteres i ettertid. Systemet må ha en så god kvalitet at nødvendige detaljer fanges opp og i etter tid kan vises for de formål som her er angitt.

Systemet skal effektivt varsle døgnbetjent vaktentral, driftssentral, eller liknende vaktordninger som sikrer at personell som er kompetent til å følge opp den uønskede situasjoner varsles umiddelbart.

De systemer som etableres for de over nevnte formål, må ikke enkelt kunne omgås, narres eller settes ut av spill (sabotasje) uten at dette blir oppdaget. Systemene må så langt mulig også fungere i mørke og dårlig vær (vind, snø mv.).

Ved valg av system for kameraovervåkning eller liknende er det viktig å ta personvern-hensyn, holde god dialog med de ansatte, og overholde *personopplysningsloven*.

- Følge Datatilsynets regler for ”Fjernsynsovervåkning” - i henhold til *Lov om behandling av personopplysninger (personopplysningsloven)* og *forskrift om behandling av personopplysninger (personopplysningsforskriften)*.
- Det skal blant annet ved skilt eller på annen måte varsles om at overvåkning finner sted. Slik varsling skal utformes og settes opp på hensiktsmessige steder, slik at dette også gir en forbyggende effekt.
- Vi viser også til at det normalt kun er tillatt å oppbevare opptak i sju dager. Men det finnes relevante unntak - blant annet dersom det er sannsynlig med politi-etterforskning, eller av forsvarsmessige hensyn.
- Det kan vurderes helt eller delvis å deaktivere funksjoner for bildeopptak og lagring når anlegget er betjent, forutsatt at nødvendig oppmerksomhet vises, og det er pålitelige mekanismer for å aktivere systemet når anlegget forlates.

Det skal etableres ordninger for rask utrykning av kompetent personale. Rask reaksjon skal også omfatte en vurdering av bruk av ulike andre metoder for å varsle og anrope uvedkommende. Dette kan for eksempel omfatte kombinasjoner av å tenne lys, bevegelige lyskastere, alarmsignal/ sirener, talemeldinger og toveiskommunikasjon.

Det skal i tillegg være gjennomførbare planer for skjerpet overvåkning av anlegget i ekstraordinære situasjoner.

De mekanismene (systemene) som velges bør være fleksible med hensyn til behov for utvidelse, tilkobling av nye elementer og teknologisk utvikling. Videre bør løsningene som velges være fleksible med hensyn til behov for endringer som følge av driftsmessig og operativ utvikling, samt erfaringer (hendelser og øvelser).

Det skal legges til rette for varsling av og samarbeid med politi, andre nødetater og forsvar, herunder at disse kan benytte de over nevnte mekanismer i forbindelse med utrykning, vakthold, etterforskning eller andre innsatser.

Del III Effektiv gjenoppretting og reparasjonsberedskap

5.III.1 Generelle krav

§ 4-1 Reparasjonsberedskap, § 4-3. Drift i ekstraordinære situasjoner og gjenoppretting av funksjon og § 4-5 Materiell og utstyr- jf § 4-5 Transport.

5.III.2 Spesifikke krav til gjenoppretting og reparasjonsberedskap etter anlegg og klasse

§ 5-4. Sikringstiltak for klasse 1

- | | |
|----|--|
| 2. | Skader skal utbedres og anleggets funksjoner skal gjenopprettes uten ugrunnet opphold. |
|----|--|

Vedlegg 1

1.1	<i>For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg gjelder følgende krav:</i>
------------	--

- | | |
|-------|--|
| 1.1.5 | Det skal være tilgang på reserver for viktige komponenter. |
|-------|--|

§ 5-5. Sikringstiltak for klasse 2

- | | |
|----|---|
| 2. | Vitale funksjoner skal opprettholdes i ekstraordinære situasjoner og anleggets funksjonalitet skal gjenopprettes uten ugrunnet opphold. |
|----|---|

Vedlegg 2 – krav etter punkt 2.1.

2.1.	<i>For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:</i>
-------------	--

- | | |
|----------|--|
| 2.1.1 c. | Gjenoppretting av eventuelle funksjonstap skal skje uten ugrunnet opphold. |
|----------|--|

§ 5-6. Sikringstiltak for klasse 3

- | | |
|----|---|
| 2. | Vitale funksjoner skal opprettholdes i ekstraordinære situasjoner og anleggets funksjonalitet skal gjenopprettes uten ugrunnet opphold. |
|----|---|

Vedlegg 3 – krav etter punkt 3.1.

3.1	<i>For transformatorstasjoner, koblingsanlegg/-stasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:</i>
------------	--

- | | |
|----------|--|
| 3.1.1 c. | Gjenoppretting av eventuelle funksjonstap skal skje så raskt som fysisk mulig. |
|----------|--|

5.III.3 Hensikten med bestemmelsene

Dersom det på tross av sikrings- og beredskapstiltak skulle opptre svikt i eller hindring av funksjon må gjenoppretting av funksjon skje raskt for å redusere konsekvensene av svikten. Dersom kraftanlegg skades, må de utbedres og føres tilbake til normal stand så raskt som mulig, eventuelt forsterkes og fornyes, slik at nye utfall eller liknende kan forebygges eller forhindres.

5.III.4 Nærmere om krav til effektiv gjenoppretting og reparasjonsberedskap

Energiloven kapittel 9 Beredskap stiller i § 9-2 Beredskapstiltak krav til gjenoppretting av normal situasjon. Dette gjelder både funksjon, system og det enkelte anlegg

Når det gjelder kravene til gjenoppretting, reparasjonsberedskap mv. viser vi til § 4-1 Reparasjonsberedskap, § 4-3 Drift i ekstraordinære situasjoner og gjenoppretting av funksjon og § 4-5 Materiell og utstyr. I tillegg har klassifiserte anlegg noen særlige krav til reparasjonsberedskap og gjenoppretting etter §§ 5-4, 5-5 og 5-6.

Gjenoppretting omfatter i mange tilfeller reparasjon eller gjenanskaffelse av tunge komponenter med lange leveringstider. Det er derfor viktig at gjenoppretting planlegges nøye med hensyn til hvordan ulike komponenter kan erstattes, transporteres og midlertidige improvisasjoner kan utføres.

Selv om havari/ utfall av en viktig komponent eller anleggsdel ikke nødvendigvis fører til strømutfall eller andre umiddelbare konsekvenser av vesentlig betydning, svekker det redundansen og fleksibiliteten i systemet. Dette kan få alvorlige følger dersom nye feil eller ekstraordinære situasjoner inntreffer. Tiltak skal derfor ikke bare gjøres ut fra isolerte vurderinger av enkeltfeil, men ut fra systemmessige vurderinger av muligheten for at det kan oppstå flere samtidige hendelser. Av samme grunn må gjenopprettingen etter betydelige havarier starte så snart som overhodet mulig.

Denne bestemmelsen pålegger ingen å gjennomføre risikofylte oppdrag med fare for eget liv og helse. Ved begrunnet mistanke (jf. verifikasjon av hendelsen) om at en risikabel situasjon er under utvikling, skal det ventes på tilstrekkelige forsterkninger, eventuelt fra vedkommende nødetat. Vi forutsetter at ansvarlige personer og personell på stedet utviser skjønn.

Del IV Redundans i anlegg og system

5.IV.1 Generelle krav til redundans

For generelle krav til redundans etter anlegg og klasse – se blant annet:

Klasse 2 – Vedlegg 2 – krav etter punkt 2.1.

Klasse 3 - Vedlegg 3 – krav etter punkt 3.1.

Nærmere om redundans i anleggenes egen strømforsyning (stasjonsstrøm), se del V Anleggenes egen strømforsyning, som må ses i sammenheng med dette punkt om redundans (kabler og lignende) i anlegget.

Det er ikke spesifikke krav til redundans i klasse 1-anlegg. Det må vurderes i det enkelte tilfelle – jf § 5-8 Analyse.

5.IV.2 Spesifikke krav til transformatorstasjoner og koblingsstasjoner i klasse 2 om redundans

2.2.	<i>For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
2.2.5	Anlegget skal ha dublerede føringer for stasjonsstrøm og styresignaler.
2.2.6	Skal som hovedregel ha dublering av de viktigste komponenter for anleggets primære funksjoner. Dette gjelder bl.a. samleskinner, skillebrytere, samt annen nødvendig utrustning.

- 2.2.8 Viktige kabler for driftskontroll og styre- og nødstrøm skal så langt som mulig, fysisk separeres fra høyspentkabler.

5.IV.3 Spesifikke krav til kraftstasjoner klasse 2 om redundans

- 2.3** *For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:*
- 2.3.7 Anlegget skal som hovedregel ha dublering av de viktigste komponenter og annen nødvendig kontrollutrustning, samt ha dublerede føringer for stasjonsstrøm og styresignaler. Det kreves ikke redundans for anleggets hovedkomponenter, som turbin, generator mv.
- 2.3.9 Viktige kabler for driftskontroll og styre- og nødstrøm skal så langt som mulig fysisk separeres fra høyspentkabler

5.IV.4 Spesifikke krav til driftskontrollsystem klasse 2 om redundans

- 2.4** *For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 2.1:*
- 2.4.1.3 Viktige komponenter og systemer skal ha redundans slik at én enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 2.4.2.5 Anlegget skal også oppfylle kravene som fremgår av kapittel 7.

5.IV.5 Spesifikke krav til transformatorstasjoner og koblingsstasjoner i klasse 3 om redundans

- 3.2.** *For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i over nevnte punkt 3.1:*
- 3.2.7 Anlegget skal ha dublerede og fysiske uavhengige kabelføringer for hhv. styring og samband, nød- og stasjonsstrøm og høyspent, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 3.2.8 Anlegget skal som hovedregel ha dublering av de viktigste komponenter for anleggets primære funksjoner. Dette gjelder bl.a. samleskinner, effekt- og skillebrytere, samt annen nødvendig utrustning. Hovedtransformatorers funksjon skal ha redundans i anlegg eller system.
- 3.2.10 Dublering etter punkt 3.2.7 til 3.2.9 skal så langt som mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.

5.IV.6 Spesifikke krav til kraftstasjoner klasse 3 om redundans

- 3.3** *For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:*
- 3.3.5 Anlegget skal ha dublerede og fysiske uavhengige kabelføringer for hhv. styring og samband, nød- og stasjonsstrøm og høyspent, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 3.3.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk

	og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.
3.3.8	Det kreves ikke redundans for anleggets hovedkomponenter, som turbin, generator mv.

5.IV.7 Spesifikke krav til driftskontrollsystem klasse 3 om redundans

3.4	<i>For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 3.1:</i>
3.4.1	<i>Driftssentraler</i>
3.4.1.5	Alle komponenter og systemer skal utføres fullredundant med bl.a. dublerter og fysiske uavhengig prosessutstyr, føringsveier for strøm, signaler og sambandsutrustning, samt annen nødvendig utrustning, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
3.4.1.7	Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres
3.4.2.4	Anlegget skal også oppfylle kravene som fremgår av kapittel 7.

5.IV.8 Hensikten med bestemmelsene

Viktige kraftforsyningsanlegg skal innrettes og utrustes slik at én enkelt feil eller hendelse ikke skader eller hindrer anleggets vitale funksjoner i det kraftsystemet det er en del av.

5.IV.9 Nærmere om krav til redundans i anlegg eller system

Kravene innebærer at det skal finnes andre komponenter eller deler av anlegget som automatisk eller ved rask manuell omkobling eller annen inngripen kan overta funksjon til den anleggsdelen som har feil eller er ødelagt. En metode for å oppnå slik redundans, er å ha dobbelt sett (jf. alternativer) av viktige komponenter (for eksempel hoved-transformatorer, samleskinner og brytere) – gjerne i kombinasjon med fysisk og elektrisk atskillelse enten ved avstand eller fysisk beskyttelse. Eksempelvis kan man plassere (minst) to hoved-transformatorer (for et gitt spenningsnivå) i hver sin transformatorcelle, som hver for seg kan ta den normallasten anlegget er dimensjonert for. Sannsynligheten for at begge havarerer (f.eks. ved brann) samtidig, blir da svært liten.

Alternativt kan redundans ordnes ved at et annet anlegg kan overta det vesentlige av funksjonen til et havarert anlegg – for eksempel at det finnes to alternative innføringsstasjoner i et forsyningsområde. Merk at dette er en lokal parallell til, men ikke helt det samme som et mer overordnet N-1 systemkrav til ordinær driftssikkerhet.

Manglende redundans kan i noen grad kompenseres ved å øke evnen til rask gjenoppbygging ved for eksempel en planlagt og fysisk forberedt forbi-/omkobling.

For alle klasse 3-anlegg - legges både viktige strøm- og styrekabler i hver sine egne fysisk separate traséer.

For driftskontrollsystem, se også veiledning til kapittel 7 Driftskontrollsystem.

Anlegg i klasse 2 og 3 skal utstyres med effektive vern og overspenningsavledere. Når det gjelder tiltak for å forhindre teknisk svikt og annen skade, viser vi til:

- *Energilovforskriften* § 3-5. Plikter ved konsesjon for elektriske anlegg a) Drift, vedlikehold og modernisering.
- *Forskrift om systemansvaret i kraftsystemet (FoS)* – med veiledning utgitt av Statnett.
- *Forskrift om elektriske forsyningsanlegg* - med veiledning fastsatt av DSB.
- *Forskrift om kvalifikasjoner for elektrofagfolk*.

5.IV.10 Nærmere om krav til redundans i eksisterende anlegg i klasse 2 og 3

Med unntak av ovennevnte hjelpesystemer kreves det normalt ikke ombygging eller anskaffelse av tyngre komponenter for å oppnå redundans. Manglende redundans må i så fall søkes kompensert ved blant annet beredskapsplaner og reparasjonsberedskap. For eksempel skal det foreligge en konkret plan for hvordan hovedtransformatoren kan erstattes av en annen. Ved manglende redundans (brytere, samleskinne og liknende) i koblingsanlegget skal det foreligge planer, utstyr, reservedeler og kompetanse for rask forbikobling til ordinær gjenoppretting har funnet sted.

Del V Anleggenes egen strømforsyning, nødstrøm

Funksjonelle krav - se

Klasse 2 – Vedlegg 2 – krav etter punkt 2.1.

Klasse 3 - Vedlegg 3 – krav etter punkt 3.1.

5.V.1 Hensikten med bestemmelsene

Bestemmelsene gir både funksjons- og konkrete systemkrav til anleggenes egen strømforsyning og nødstrøm (stasjonsstrøm), slik at anleggene med nødvendig hjelpeutstyr kan fortsette å fungere selv om oppstår feil i eget anlegg og utfall av ordinær strømforsyning. Anleggene skal også kunne betjenes så lenge det er forsvarlig og bidra til å oppfylle HMS krav dersom et anlegg må evakueres eller liknende.

5.V.2 Generelle krav til anleggenes egen strømforsyning, nødstrøm

For alle klassifiserte anlegg og særlig anlegg i klasse 2 og 3, må anleggenes egen strømforsyning (inkludert nødstrøm) – stasjonsstrøm - vies stor oppmerksomhet. Denne må planlegges og utføres slik at den er tilstrekkelig robust og virker til en hver tid.

Herunder må også *FEF* og veiledningen til kapittel 4 Høyspenningsinstallasjoner i *FEF*, følges. Videre finnes relevante krav og veiledning i Norsk elektroteknisk norm *Elektriske lavspenningsinstallasjoner* utgitt av NEK.

Ved vurdering av behovet for nødstrøm må det blant annet tas hensyn til følgende forhold:

- Hele driftskontrollsystemets betydning og klasse, også kontrollfunksjonene ute i det enkelte anlegg.
- De ulike anleggs, komponenters og sambandsveiers betydning for driftskontrollfunksjonene.
- Vedkommende anleggs tilknytning til det lokale/regionale strømmettet og kvaliteten på dette.
- Anleggenes utstyr, interne forhold og egenforbrukets art (maksimal last, forbruk i feilsituasjoner, motorlast/ vekselretter og liknende).
- Geografiske, topografiske og værmessige forhold (avsides eller sentral beliggenhet).
- Betjeningsforhold og tilgjengelighet i forhold til veiforbindelse med mer.
- Mulighetene til å føre fram og etterfylle diesel til faste og mobile nødstrømsaggregater må beregnes og planlegges, også når forholdene gjør tilgjengelighet vanskelig.
- Ved alle anlegg må det foretas en gjennomgående systemtenkning og totalvurdering (ROS) av strømforsyningen, se § 5-8 Analyse.

5.V.3 Drift og gjenopprettingsevne, kontroll og vedlikehold

For anlegg i alle klasser gjelder at anleggenes egne strømanlegg med nødstrømsforsyning skal plasseres og konstrueres slik at risikoen for skade og uhell blir minst mulig. De må kunne tåle de maksimalbelastningene de kan bli utsatt for og dessuten kunne forsyne nødvendige hjelpesystemer som for eksempel nødlys, vern og kjøling. Normalt bør det legges opp prioriterte kurser for de viktigste funksjonene som styrestrøm, kontrollrom og belysning i viktige deler av anlegget.

Anleggenes egne strømanlegg med nødstrømsforsyning skal til enhver tid holdes i forsvarlig og driftsklar stand. Ved jevne mellomrom skal funksjon, kapasitet/yteevne og utholdenhet testes. Minst én gang i året bør nødstrømsanlegget testes fullt ut med all prioritert last og ved at ordinær strømforsyning kobles fra. Det vises for øvrig til § 4-1 Reparasjonsberedskap og § 4-3 Drift i ekstraordinære situasjoner og gjenoppretting av funksjon.

5.V.4 Anleggenes strømforsyning og nødstrøm, kraftanlegg - Klasse 1

- | | |
|------------|---|
| 1.1 | <i>For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg gjelder følgende krav:</i> |
| 1.1.4 | For egen stasjonsstrømforsyning skal anlegget ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Et mobilt aggregat må kunne kobles til innenfor batteritiden. Anlegget må samlet sett ha en gangtid på minst ett døgn. |

- | | |
|------------|--|
| 1.2 | <i>For driftskontrollsystemer gjelder følgende krav</i> |
|------------|--|

1.2.1 Driftssentraler

- 1.2.1.4. Skal være utstyrt med avbruddsfri strømforsyning og mulighet for tilkobling av mobilt nødstrømsaggregat, med en samlet gangtid på minst ett døgn.

1.2.2 Sambandsanlegg

- 1.2.2.3 Anlegget skal utstyres med nødstrøm med automatisk start og gangtid på minst ett døgn.

Disse bestemmelsene styrker kravene til nødstrøm for alle nevnte anlegg i klasse 1. Samlet skal batterianlegg og nødstrømsaggregat gi en strømforsyning uten avbrudd i minst ett døgn. Nødstrømsanlegget må ha kapasitet til å opprettholde anleggets viktigste funksjoner. Tilkoblingen for nødstrømsaggregatet må forberedes, og aggregatet må alltid være så tilgjengelig at det faktisk kan kobles til før batteriene tar slutt. Utholdenhet vil blant annet være avhengig av at det etableres rutiner for etterfylling av drivstoff og annet vedlikehold. Utover dette må den som eier selv vurdere kapasitet og utholdenhet ut fra anleggets art og betydning, samt sannsynligheten for utfall i ordinær strømforsyning og konsekvenser av dette. På utsatte steder og hvor ekstraordinære forhold kan gi langvarige utfall (jf ekstremvær som "Dagmar"), må lenger utholdenhet vurderes.

For driftssentraler skal de systemene som har betydning for driften av kraftsystemet, forsynes fra batterianlegg/UPS (Uninterruptible Power Supply) som bør ha en driftstid på minst 2 timer. Et mobilt nødstrømsaggregat må uansett kunne kobles til innen den driftstid batterianlegget gir.

Dersom driftsentralen er lokalisert sammen med KBO-enhetens administrasjon og ledelse bør permanent nødstrømsaggregat vurderes.

Sambandsanleggene bør utstyres med batterianlegg med driftstid ½ -1 døgn eller mer, avhengig av tilgjengelighet. Det bør uansett planlegges og forberedes tilkobling av nødstrømsaggregat.

5.V.5 Anleggenes strømforsyning og nødstrøm - kraftanlegg klasse 2

5.V.5.1 Funksjonelle krav – alle anlegg

2.1. For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:

- 2.1.3 Anlegget skal fungere uavhengig av de strømutfall som kan forekomme i ordinær strømforsyning og påregnelige feil i eget strømforsyningssystem

5.V.5.2 Spesifikke krav

2.2. For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:

- 2.2.7 Skal ha et dublert nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Om det ikke er installert et stasjonært nødstrømsaggregat, må et mobilt aggregat kunne kobles til innenfor batteritiden under maksimal belastning. Anlegget må samlet sett ha en gangtid på minst to døgn.

2.3	<i>For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
2.3.8	Skal ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Om det ikke er installert et stasjonært nødstrømsaggregat, må et mobilt aggregat kunne kobles til innenfor batteritiden under maksimal belastning. Anlegget må samlet sett ha en gangtid på minst to døgn.

2.4	<i>For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
2.4.1	<i>Driftssentraler</i>
2.4.1.5	Driftssentralens data-, sambands- og øvrige systemer som er nødvendige for driften av kraftsystemet, skal forsynes fra to uavhengige strømkurser. Dette inkluderer et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning som skal en driftstid på minst seks timer. Dersom det ikke er installert permanent nødstrømsaggregat, skal et mobilt nødstrømsaggregat kunne kobles til og være tilgjengelig godt innenfor batterikapasiteten. Nødstrømsanlegget skal samlet sett ha automatisk start og gangtid på minst to døgn.
2.4.2	<i>Sambandsanlegg:</i>
2.4.2.4	Anlegg med god tilgjengelighet skal utstyres med nødstrøm med automatisk start og gangtid på minst to døgn. For vanskelig tilgjengelige anlegg skal inntil 14 døgn vurderes.

Anleggene skal fungere uavhengig av både strømutfall som kan forekomme i ordinær strømforsyning og påregnelige feil i eget strømforsyningssystem. Dette betyr at anleggene skal ha egne pålitelige nødstrømssystemer som alltid fungerer og kan overta nødvendige funksjoner dersom den ordinære strømforsyningen faller ut.

Anleggene må fungere under samtidig bortfall av nettstrøm og feil i eget anlegg. Det betyr at eget strøm/-nødstrømsanlegg må bygges elektrisk redundant (unngå "single point of failure"). Dimensjonering og utholdenhet kan baseres på lokal erfaring og feilstatistikk. Det må utføres en grundig og dokumenterbar vurdering (analyse) av så vel stasjonens eget elektriske anlegg som forsyningssikkerheten i det strømnettet stasjonen er tilkoblet. I tillegg til relevant lokal avbruddsstatistikk, må det også brukes et overordnet skjønn. Overbelastninger, varmgang, kortslutninger, branntilløp, overspenninger, komponentfeil, graveuhell og et nødstrømsaggregat med startvansker er eksempler på påregnelig feil i et elektrisk anlegg. Som et minimum skal det uansett være 2 døgns selvstendig driftstid/automatisk gange.

I utgangspunktet er punkt 2.1 i vedlegg 2 til bfe et overordnet funksjonelt krav. I de etterfølgende bestemmelsene i dette vedlegget til forskriften er det stilt mer spesifikke krav. Dersom disse følges, vil det funksjonelle kravet langt på vei være oppfylt, men det må også foreligge en vurdering som fanger opp lokale særegenheter og risiko.

Driftssentralens data-, sambands- og øvrige systemer som er nødvendige for driften av kraftsystemet, skal forsynes fra to uavhengige strømkurser. Dette inkluderer batterianlegg/UPS som skal ha en samlet driftstid på minimum 6 timer. Et mobilt

nødstrømsaggregat skal kunne kobles til og være tilgjengelig innenfor driftstiden for batteriet. Driftstid for batterianlegget kan reduseres til minimum 3 timer dersom det er installert et stasjonært nødstrømsaggregat. Det må her tas hensyn til den påregnelig tid for feilretting om aggregatet ikke starter. Man skal vurdere å dublere batteri-/ UPS-systemet helt eller delvis. Dimensjonerende belastning må også vurderes.

Dersom driftsentralen er lokalisert sammen med KBO-enhetens administrasjon og ledelse, skal enheten vurdere å installere permanent nødstrømsaggregat.

Vanskelig tilgjengelige sambandsanlegg (fjelltopper og liknende) utstyres vanligvis med batterianlegg med driftstid på minst 1 til 2 døgn og stasjonært nødstrømsaggregat med gangtid inntil 14 døgn avhengig av muligheter for tilsyn/ vedlikehold og etterfylling av diesel. Alternativt kan stasjonen ha batterianlegg med driftstid på minst 2 til 3 døgn og være forberedt for tilkobling til mobilt nødstrømsaggregat. Dersom anlegget har god fysisk tilgjengelighet, kan kravene reduseres.

Sambandsanlegg i lavlandet med god tilgjengelighet bør ha batterianlegg/ UPS med driftstid på 1 til 2 døgn og være forberedt for tilkobling til et tilgjengelig mobilt nødstrømsaggregat innen batteritiden slik at minstekravet samlet sett oppfylles.

Ovennevnte skal vurderes og dokumenteres i hvert enkelt tilfelle.

5.V.6 Anleggenes strømforsyning og nødstrøm - kraftanlegg klasse 3

5.V.6.1 Funksjonelle krav – alle anlegg

3.1	<i>For transformatorstasjoner, koblingsanlegg/-stasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:</i>
3.1.3	Anlegget skal fungere uavhengig av ordinær strømforsyning og feil i anleggets eget strømforsyningssystem. Funksjon skal opprettholdes også ved upåregnelige og langvarige strømutfall.

5.V.6.2 Spesifikke krav

3.2.	<i>For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i over nevnte punkt 3.1:</i>
3.2.9	Anlegget skal ha et elektrisk og fysisk dublert system for egen stasjonsstrøm med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften av stasjonen forsynes fra to helt uavhengige og separerte strømkurser-/ systemer. Dette skal også omfatte et nødstrømssystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning og minimum har en samlet driftstid på minst seks timer. Det skal være installert et stasjonært nødstrømsaggregat med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømrubd og minst tre døgn selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Nødstrømssystemet skal tåle de maksimalbelastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling av nødvendig utstyr og liknende.
3.2.10	Dublering etter punkt 3.2.7 til 3.2.9 skal så langt som mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk

seksjonering gjennomføres.

3.3 For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:

- 3.3.6 Skal ha et elektrisk og fysisk dublert system for egen stasjonsstrøm med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften av stasjonen, forsynes fra to uavhengige og separerte strømkurser-/systemer. Dette skal også omfatte et nødstrømssystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning, og minimum har en samlet driftstid på minst seks timer. Stasjonen skal være utstyrt med en stasjonær selvdrevet anordning for stasjonsstrøm (nødstrømsaggregat, hjelpegenerator eller lignende) med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrytning og minst tre døgn selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom den stasjonære anordning skulle svikte. Nødstrømssystemet skal tåle de maksimalbelastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling og lignende.
- 3.3.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.

3.4 For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 3.1:

3.4.1 Driftssentraler

- 3.4.1.6 Skal ha et elektrisk og fysisk dublert system for egen strømforsyning med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften forsynes fra to uavhengige og separerte strømkurser-/systemer. Dette skal også omfatte et nødstrømssystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning, og minimum har en samlet driftstid på minst seks timer. Det skal være installert et stasjonært nødstrømsaggregat med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrytning og minst tre døgn selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Nødstrømssystemet skal tåle de maksimale belastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling av nødvendig utrustning, og lignende.
- 3.4.1.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres

3.4.2 Sambandsanlegg:

- 3.4.2.3 Anlegg med god tilgjengelighet året rundt skal utstyres med nødstrøm med automatisk start og gangtid på minst tre døgn, men for vanskelig tilgjengelige anlegg må dette etter forholdene økes til 30 døgn.

Overnevnte kraftanlegg skal fungere uavhengig av ordinær strømforsyning og feil i anleggets eget strømforsyningssystem. Funksjonen skal opprettholdes også ved upåregnelige og langvarige strømutfall.

Det innebærer at i tillegg til de kravene som gjelder for klasse 2 anlegg, skal anlegg i klasse 3 bygges for å forebygge og forhindre konsekvenser av både uvanlige feil (internt og eksternt) og utfall i normal strømforsyning av mange døgns varighet. Dette krever at man nøye vurderer alle mulige slags situasjoner som kan inntreffe, og hvordan disse kan forbygges og forhindres ved det elektriske og andre opplegg man velger, både med hensyn til planlegging, drift, sikringstiltak og vedlikehold.

Kraftanleggets eget strømforsynings- og nødstrømsanlegg må bygges helt redundant med både fysisk, elektronisk og elektrisk separasjon (unngå alle "single point of failure"). Dette gjelder også kabelføringer (eksempelvis brann) hvor høyspent, lavspent og svakstrøm (styrestrøm) må skilles fysisk (brannmotstand minst EI 60), eller ved god avstand i separate føringer.

Det må bygges slik at delsystemene i det redundante systemet hver for seg har tilstrekkelig momentan kapasitet (effekt) og utholdenhet. Som et minimum skal det være 3 døgn selvstendig driftstid. Ved dimensjonering skal det tas hensyn til at langvarige strømutfall i Norge lokalt har vart i opptil 5 til 6 døgn, og i utlandet opptil flere uker over større områder (for eksempel orkanen Gudrun i Sverige).

De må forsynes fra to ordinære og innbyrdes uavhengige strømforsyninger. IKT og øvrige systemer som er nødvendig for driften av stasjonen, bør som et minimum forsynes fra batterianlegg/ UPS med en driftstid på 12 timer. Det skal være installert et stasjonært nødstrømsaggregat med automatisk oppstart ved strømbrytning og som deretter bør ha minimum 3 døgns selvstendig gangtid. Et mobilt nødstrømsaggregat skal raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Strømforsyningen skal dubleres og batterisettene med videre plasseres i separate rom. Nødstrømssystemet må kunne tåle de maksimalbelastningene det kan bli utsatt for, herunder hjelpesystemer som kjøling.

I tillegg kommer krav til gjenoppretting (se både § 5-6 punkt 3.1.1 og §§ 4-1 og 4-3), både i nett og i eget anlegg. Det vil si at når feil inntreffer, må gjenopprettingen begynne straks og man må ha planer, kompetanse og øvrige ressurser for dette. Eksempelvis er lange nok batteritider viktige for å ha tilstrekkelig tid til retting dersom feil inntreffer.

Driftssentralens data-, sambands- og øvrige systemer som er nødvendige for driften av kraftsystemet, skal forsynes fra to fysisk, elektrisk og elektronisk uavhengige strømkurser-/ systemer. Dette inkluderer også dublering med uavhengige batterianlegg/ UPS. siden det kan oppstå feil eller uhell i selve batteribanken, rommet de står i eller i tilkoblingen. Slikt kan inntreffe nettopp i en situasjon med strømutfall, når batterianlegget presses hardt og unormalt, og enheten trenger nødstrøm som mest. For klasse 3-anlegg er det derfor et krav om dublerede batteribanker i separate rom.

Batteribankene må ha opplegg for krysskobling, slik at hele batterikapasiteten kan utnyttes ved eventuelle feil i nødstrømssystemet.

Batterianleggene/ UPS skal som et minimum ha en driftstid på minst 6 timer. Det skal være installert et stasjonært nødstrømsaggregat med automatisk oppstart ved strømbrytning og som deretter bør ha minimum 3 døgns selvstendig gangtid. Et mobilt

nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Nødstrømsystemet må kunne tåle de maksimalbelastningene det kan bli utsatt for, også hjelpesystemer som kjøling og liknende.

I tillegg er det gunstig med dublert innmating fra to ulike punkter i det lokale distribusjonsnett, samt at innmatingen utføres med minst én jordkabel. Dette skal vurderes ut fra lokale forhold.

Viktige og vanskelig tilgjengelige sambandsanlegg (for eksempel radiolinjestasjoner (RL) på fjelltopper med mer) bør som et minimum utstyres med batterianlegg/ UPS med driftstid på 3 til 4 døgn og stasjonært nødstrømsaggregat med automatisk gangtid på 30 døgn. Dersom anlegget har gunstig beliggenhet med god fysisk tilgjengelighet året rundt, kan dette reduseres.

Sambandsanlegg i lavlandet med god tilgjengelighet skal ha batterianlegg/ UPS med driftstid på minst 3 døgn og nødstrømsaggregat eventuelt eller forberedt for tilkobling til et tilgjengelig mobilt aggregat.

Dette skal vurderes og dokumenteres i hvert enkelt tilfelle.

5.V.7 Nærmere om krav til nødstrøm ved eksisterende anlegg

Alle klasser

Forskriftens funksjonelle krav til kraftforsyningsanleggenes egen strømforsyning inkludert nødstrøm, og til driftskontrollanleggenes styresystemer, er av stor viktighet. Som hovedregel skal derfor forskriftens krav oppfylles for vedkommende anlegg og klasse, med nødvendige tillemper etter anleggets art og utforming. Alle anlegg må gjennomgå regelmessig, og nødvendige utbedringer foretas.

Klasse 2 og 3

For klasse 2 og 3 er hovedkravet at én enkelt feil eller hendelse ikke kan sette funksjonen, og dermed kraftforsyningsanlegget eller noen av dets vitale komponenter ut av spill. På dette punktet må anleggene gjennomgå, og åpenbare svakheter rettes. Batteribank med tilstrekkelig kapasitet må være installert og nødstrømsaggregat må kunne kobles til.

Klasse 3

For klasse 3-anlegg må minst både viktige strømkabler og styrekabler legges i hver sine egne fysisk separate traseer. Batteribankene må oppgraderes til å holde de brukstider som er gitt i denne forskrift og bør dubleres i separate rom. Nødstrømsaggregat må være installert eller tilgjengelig på kort varsel.

Del VI Kompetent bemanning av anlegg

5.VI.1 Generelle krav til kompetent bemanning av anlegg

Energiloven § 9-1, 3. ledd lyder:

”Alle enheter i KBO skal sørge for at virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver etter dette kapittelet”.

Se også forskriftens § 4-2 Kompetanse og personell. For driftskontrollsystemer, se også Kapittel 7 Beskyttelse av driftskontrollsystemer.

5.VI.2 Hensikten med bestemmelsene

I ekstraordinære situasjoner ved for eksempel svikt i driftssentralen eller fjernstyringen, må viktige anlegg kunne betjenes ved hjelp av lokal kontroll. Betjeningen kan i en del situasjoner også være et tiltak for å holde nødvendig oversikt over anlegget fysisk eller elektrisk, ved lokale havarier eller i forbindelse med vakthold.

5.VI.3 Nærmere om krav til kompetent bemanning av anlegg

Vi krever at KBO-enheten skal kunne drifte sine anlegg med kompetent personell. Hensiktsmessigheten av å bemanne anlegg ordinært eller ekstraordinært må vurderes lokalt i hvert enkelt tilfelle. Dette skal nedfelles i enhetens beredskapsplan.

For driftskontrollsystemer gjelder særlige krav etter forskriftens kapittel 7.

Bestemmelsene i denne paragrafen stiller krav til at bemanning av anlegg skal være mulig ved hjelp av planer og tilgjengelige kapasiteter (antall, opplæring, øvrige ressurser og øvelser). Eksempler på situasjoner som kan kreve ekstraordinær bemanning:

- Feil/skader og driftsforstyrrelser i anlegg/system.
- Bortfall av automatiske driftskontrollfunksjoner, anlegg må styres lokalt.
- Beredskapssituasjoner som krever særlig vakthold/årvåkenhet og beredskapsmessige forberedelser.
- Etter vedtak (for eksempel erklært beredskap) fra sentral myndighet.

Med kompetanse menes både nødvendig kunnskap om anlegget, hvordan det lokalstyres og formell kompetanse i forhold til selvstendig adgang til høyspentanlegg, se *forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg*.

Det er ikke stilt noen eksplisitte krav til utholdenhet, men dersom det oppstår en situasjon som krever ekstraordinær bemanning av anlegg, må man regne med at denne kan vare en stund inntil mer normal drift er gjenopprettet eller situasjonen for øvrig har normalisert seg. Det bør planlegges for minst 2 døgn med et opplegg for logistikk og avløsning, som eventuelt kan forlenges. Vi forutsetter at hensynet til arbeidstidsbestemmelser og liknende blir ivare tatt.

I det etterfølgende gir vi i tillegg en mer spesifikk veiledning i forhold til klasse.

5.VI.4 Krav til kompetent bemanning av anlegg i klasse 1

Utover generelle krav og *forskrift om krav til kompetanse med videre hos anleggs- og områdekonsesjonærer (kompetanseforskriften)*, er det ikke spesifikke krav til kompetent

bemanningsav klasse 1-anlegg. Dette må vurderes i det enkelte tilfellet, jf § 5-8 Analyse. Vi forutsetter imidlertid at man har tilgang til den bemanningen og kompetansen som skal til for å håndtere ekstraordinære situasjoner.

5.VI.5 Spesifikke krav til kompetent bemanning av kraftforsyningsanlegg i klasse 2

2.1.4	Anlegget skal kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriften, jf. § 4-2.
-------	--

Tiltaket skal planlegges av vedkommende enhet i KBO, som skal ha nødvendige kapasiteter, antall, opplæring, øvrige ressurser og øvelser for dette.

5.VI.6 Spesifikke krav til kompetent bemanning av kraftforsyningsanlegg i klasse 3

3.1.4	Alle anlegg skal samtidig og så raskt som mulig kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriften, jf. § 4-2.
-------	--

I tillegg til krav etter klasse 2 skal alle anlegg i klasse 3 kunne bemannes samtidig og så raskt som mulig.

Med begrepet ”så raskt mulig” har vi tatt hensyn til at det mange steder kan være store avstander, og at aktuelt personell i utgangspunktet kan være opptatt andre steder med andre viktige gjøremål, eller må innkalles. Berørte anlegg bør likevel kunne bemannes i løpet av få timer. I forhold til meget omfattende situasjoner må selskapet ha vurdert dette i sine risikovurderinger og ha en gjennomtenkt beredskap/prioritering.

Del VII Krav til alternativ drift og beredskapsrom

5.VII.1 Driftskontrollsystemer klasse 1

1.2	<i>For driftskontrollsystemer gjelder følgende krav:</i>
-----	--

1.2.1	<i>Driftssentraler</i>
-------	------------------------

1.2.1.5	Skal ha et alternativt opplegg for utøvelse av viktige funksjoner for drift og ledelse i en ekstraordinær situasjon.
---------	--

5.VII.2 Driftskontrollsystemer klasse 2

2.4	<i>For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
-----	--

2.4.1	<i>Driftssentraler</i>
-------	------------------------

2.4.1.6	Skal ha et alternativt opplegg for utøvelse av alle viktige funksjoner i en ekstraordinær situasjon.
---------	--

5.VII.3 Driftskontrollsystemer klasse 3

3.4	<i>For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt</i>
-----	---

3.1:

3.4.1 Driftssentraler

- 3.4.1.8 Skal ha et beredskapsrom og/ eller fysisk alternativ sted med opplegg for utøvelse av alle viktige funksjoner i en ekstraordinær situasjon.

5.VII.4 Hensikten med bestemmelsene

Driftskontrollsystemer må etter sin klasse (jf betydning) ha et opplegg for alternativ drift i ekstraordinære situasjoner eller andre tilfeller hvor f.eks. ordinær driftssentral svikter eller blir utilgjengelig.

For nærmere bestemmelser om reservedriftssentral mv. vises det til § 7-15 bokstav a.

5.VII.5 Driftskontrollsystemer klasse 1 og 2 – alternativ drift

Driftskontrollsystemer i klasse 1 og 2 skal ut fra sin funksjon og betydning ha et alternativt opplegg for drift, ledelse og gjenoppretting i ekstraordinære situasjoner. Det skal fungere dersom den ordinære driftssentralen havarer, må evakueres eller blir ødelagt av for eksempel brann. Ved alternativ drift skal viktige funksjoner kunne ivaretas på en sikker og effektiv måte. Det kan gjøres ved hjelp av et forberedt alternativt sted eller ved lokal betjening av aktuelle anlegg. Det er opp til den enkelte enheten å planlegge og etablere slik alternativ drift. Sambandsopplegget må være klart, og øvelser må gjennomføres, blant annet for å kontrollere at opplegget virker og for å etablere og opprettholde kompetansen i forhold til en alternativ drift.

5.VII.6 Driftskontrollsystemer klasse 3 - beredskapsrom

For driftskontrollsystemer i klasse 3 skal det være et beredskapsrom som kan tjene som en reserve- eller nøddriftssentral, dersom driftssentralen blir ødelagt ved for eksempel ødeleggelse eller havari i den ordinære driftssentralen. Beredskapsrommet skal beskytte mot hendelser som krever fysisk beskyttelse og sikre viktige funksjoner.

Reserveløsningen av et redundant system kan lokaliseres i beredskapsrommet. Dersom beredskapsrommet blir benyttet til daglig, må det sikres etter kravene som funksjonen tilsier. Beredskapsrommet skal være operativt på kort varsel. Enheten må derfor:

- Gjøre forberedelser for enkel flytting og tilkobling av sambands- og datautstyr fra den ordinære driftssentralen.
- Ha oppdaterte utstyrslistor og planer for utstyr som skal bli tilført fra andre steder.
- Sørge for sambandsveier, nødstrøm og øvrig nødvendig utstyr.
- På kort varsel kunne utstyre beredskapsrommet med de hjelpemidlene (oppdaterte kart, oversikter, sambandsutstyr og annet), som er nødvendig for å:
 - kunne lede den delen av kraftforsyningen som selskapet er ansvarlig for
 - ha løpende forbindelse med høyere og lavere ledd innenfor KBO.
 - kommunisere med øvrige relevante etater (politi, fylkesmenn og andre).

5.VII.6.1 Prosjektering

Ved prosjektering av beredskapsrom benyttes kravene til tilfluktsrom etter *forskrift om tilfluktsrom*. I tillegg skal kravene i etterfølgende tabell være oppfylt.

Plassbehov	Gassluse	Ventilasjon
Min. 2 m ² / per person.	I alle beredskapsrom. Innvendige mål minimum: L x B = 2,5 x 1,5 m	Normalventilasjon: Min. 20 m ³ /time & person Filterventilasjon: Min. 10 m ³ /time & person.

Nødstrømsforsyning med batterier eller dieselaggregat skal vurderes i hvert enkelte tilfelle, se kravene til nødstrøm for driftssentral i klasse 3 i vedlegg 3 til bfe, punkt 3.4.1.6. Enheten må foreta sluttkontroll av tetthet, overtrykk, installasjon og andre relevante forhold.

Det skal foreligge oppdaterte utstyrslistes, og planer for utstyr som skal bli tilført.

For utstyrsliste, se vedlegg 13 til veiledningen.

5.VII.6.2 Drift og vedlikehold

Det skal være utpekt personer som er ansvarlige for drift og vedlikehold av beredskapsrommene. Den som er ansvarlig for vedlikehold, skal ved regelmessige inspeksjoner sørge for at rommenes verneevne ikke forringes. Slitte eller defekte komponenter skal utbedres, eller skiftes ut. Det skal foreligge en oversikt over rommenes inventar og utstyr. Forskrifter og bruksanvisning med norsk tekst for vifter, aggregater, batterier og annet, skal være oppslått i nærheten av objektene.

For kontroll av temperatur og fuktighet skal termometre og hygrometre plasseres på hensiktsmessige steder i anlegget. Grunntemperaturen bør ligge på ca. 15° C og den relative fuktigheten bør ikke være over 50 - 60 %.

Beredskapsrommene skal kontrolleres ved rutinemessige inspeksjoner. For anlegg i dagen, bør kontrollen utføres hvert kvartal, for fjellanlegg hver 14. dag. Inspeksjonene skal protokollføres med angivelse av tidspunkt, resultat av inspeksjonen og hva som er gjort for å rette eventuelle feil og/eller mangler.

Se vedlegg 13 til veiledningen for liste over hva som skal kontrolleres ved de rutinemessige inspeksjonene.

5.VII.6.3 Kontroll

I tillegg til de nevnte inspeksjonene skal alle beredskapsrom kontrolleres minimum én gang hvert år.

Når det ved beredskap beordres klargjøring av beredskapsrom, skal enheten gjennomføre fullstendig vedlikeholdsinspeksjon. Blant annet skal enheten funksjonsprøve og kontrollere at tekniske installasjoner virker slik det er forutsatt, og straks utbedre eventuelle mangler.

Se vedlegg 13 til veiledningen for sjekkliste for disse kontrollene.

5.VII.7 Eksisterende beredskapsrom

Nyere beredskapsrom som er etablert ifølge BfK (2002), skal som hovedregel beholdes.

Eldre beredskapsrom ble tidligere også benevnt beskyttende rom eller ”kommando- eller alarmplasser”. Disse ble i sin tid pålagt av NVE eller tidligere KSFN - Kraftforsyningens sivilforsvarsnemnd. De kan også være kombinert med tilfluktsrom etter Sivilforsvarets krav.

Kommandoplasser var tilfluktsromsliknende (beskyttende)rom/områder i administrasjonsbygg og liknende, hvor ledelse og driftspersonell kunne søke tilflukt ved krigshandlinger og liknende – der de også kunne utøve ledelsesfunksjoner.

Alarmplasser var mindre - ofte enklere utstyrte - tilfluktsrom gjerne i forbindelse med kraftanlegg (stasjoner) hvor personell (driftspersonell, montører og liknende) på samme måte kunne søke tilflukt/beskyttelse. De må ikke forveksles med redningsrom, men kan også ha en kombinert funksjon med slike.

Kommando- og alarmplasser var fram til 1990- tallet pålagt gjennom enkeltvedtak. NVE har oversikter for hvert enkelte selskap (enhet i KBO) om pålegg for anordning og kontroll av disse. Det fantes også et detaljert regelverk gitt sist (1997) ved henholdsvis ”RSK” - Retningslinjer for sikring av kraftforsyningsanlegg” (kap. 14 *Beskyttende rom*) og ”BHK” – Beredskapshåndbok for kraftforsyningen”. I nyere tid var dette regulert i BfK § 6-4 punkt f. *Beredskapsrom*, og er knyttet opp mot driftskontrollfunksjonene.

Selv om mange av de eksisterende eldre beredskapsrommene ikke hadde blitt pålagt i dag, skal likevel tidligere tiders pålagte og utførte sikringstiltak opprettholdes - gitt at de fremdeles har eller kan få en funksjon ved beredskap, ikke er for kostbare å vedlikeholde, og ikke står i veien for en hensiktsmessig utvikling (modernisering, utvidelser) av bygg og anlegg.

På en noen steder har ikke lenger nevnte ”kommando- og alarmplasser” noen vesentlig funksjon. Dette fordi det enten ikke finnes noe stedlig personell, eller de er i en slik tilstand at de neppe vil ha den tiltenkte beskyttende effekt, eller at vedkommende stasjon neppe kan tenkes å bli utsatt for relevant risiko.

Dersom et slikt beredskapsrom:

- ikke fyller noen funksjon etter denne forskriften,
- ikke også er tilfluktsrom etter Sivilforsvarets krav,
- ikke fyller noen funksjon som redningsrom for personell (ved brann o.l.),
- ikke i det øvrige kan antas å ha eller få noen vesentlig beredskapsmessig betydning for vedkommende enhet – jf. lokal ROS-analyser og beredskapsplaner,

kan de nedlegges eller omdisponeres dersom vedkommende KBO-enhet ser behov for det.

For å få dokumentert og utkvittert gamle vedtak, sendes en kort melding (oversikt) til NVE om hvilke steder dette eventuelt gjelder.

Del VIII Øvrige tiltak

5.VIII.1 Beskyttelse mot geomagnetisk induuerte strømmer

3.2 *For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i over nevnte punkt 3.1:*

3.2.11 Det skal gjøres en vurdering av konsekvensene av geomagnetisk induuerte strømmer, og iverksettes relevante tiltak for å beskytte hovedtransformatorer.

5.VIII.2 Hensikten med bestemmelsen

Hovedtransformatorer i transformatorstasjoner i klasse 3, vil som regel være sammenkoblet med lange kraftledninger, og må derfor beskyttes mot geomagnetisk induuerte strømmer (GIC) for å unngå skader og havari når slik induksjon oppstår i slike ledninger.

Ansvar for beskyttelse av transformatorene mot GIC tilligger den enkelte KBO-enhet. Denne må gjøre egne vurderinger basert på sårbarhet, betydning og beliggenhet i nettet, konstruksjon mv., og etablere tiltak og rutiner for å begrense mulige skadevirkninger av GIC.

5.VIII.3 Krav til start på svart nett og øydrift

5.VIII.3.1 Kraftstasjon klasse 2

2.3 *For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:*

2.3.10 Minst ett aggregat skal normalt kunne starte på spenningsløst nett (svart nett),

5.VIII.3.2 Kraftstasjon klasse 3

3.3 *For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:*

3.3.9 Minst ett aggregat skal normalt kunne starte på spenningsløst nett (svart nett) og kunne drives separat (øydrift).

5.VIII.4 Hensikten med krav til start på svart nett og øydrift

Alle kraftstasjoner i klasse 2 og 3 i ulike driftsområder skal kunne starte på svart nett for å kunne bygge opp sentral- og regionalnettet etter større utfall. Tilsvarende skal kraftstasjoner i klasse 3 i en ekstraordinær situasjon være stabile nok til å kunne drives separat og dermed holde nettet stabilt, i første omgang i et avgrenset område, men også ved langvarige avbrudd. Ut fra en lokal vurdering kan det også være aktuelt å ha ovennevnte beredskap også ved andre kraftverk.

5.VIII.5 Nærmere om krav til start på svart nett og øydrift

Kravet om at kraftstasjoner skal kunne starte på svart nett ("black start"-funksjonalitet) medfører blant annet krav til nødstrøm, bemanning, kompetanse og kontrollutrustning, det vil si beredskapskrav som uansett skal oppfylles ved slike stasjoner. Det kreves ikke større ombygging av generatorer som ikke er egnet for dette, eller kostbar tilleggsutrustning ved termiske kraftverk.

For øydrift skal det installeres nødvendig regulerutstyr slik at stasjonen i utgangspunktet er egnet for slik drift. Det kreves heller ikke her større ombygginger.

For krav til gjenopprettingsplan og operative drift, viser vi til *forskrift om systemansvaret i kraftsystemet (FoS)*.

Del IX Kraftledninger

5.IX.1 Kraftledning klasse 1

1.3 *For kraftledninger gjelder følgende krav:*

- 1.3.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessige betydning.

5.IX.2 Kraftledning klasse 2

2.5 *For kraftledninger gjelder følgende krav:*

- 2.5.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessig betydning.
- 2.5.2 For kabler skal i tillegg viktige komponenter som endemuffer og skjøter beskyttes. Alternativt kan det anskaffes reservekomponenter som lagres på sikkert sted, og det skal være tilgang til reservekabel med mer etter § 4-4.
- 2.5.3 Gjenoppretting av funksjonstap skal skje uten ugrunnet opphold.

5.IX.3 Kraftledning klasse 3

3.5 *For kraftledninger gjelder følgende krav:*

- 3.5.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessige betydning.
- 3.5.2 For kabler skal i tillegg viktige komponenter som endemuffer og skjøter beskyttes. Alternativt kan det anskaffes reservekomponenter som lagres på sikkert sted, og det skal anordnes reservekabel med nødvendig utstyr etter § 4-4.
- 3.5.3 Gjenoppretting av eventuelle funksjonstap skal skje så raskt som fysisk mulig.

5.IX.4 Hensikten med krav til kraftledninger i klasse 1-3

Kraftledninger etter disse bestemmelsene omfatter både luftledning og kabel i sjø og på land med tilhørende muffeanlegg.

Kraftledninger kan være utsatt for værpåkjenninger som for eksempel sterk vind, ising, salting, atmosfæriske utladninger og lynnedslag. Mange ledninger er bygd i ras- og skredutsatte områder. Mindre ledninger kan være utsatt for skade fra nærstående vegetasjon i kombinasjon med sterk vind. Mekaniske og elektriske feil som følge av langvarig slitasje og elde forekommer også. Sabotasje kan heller ikke utelukkes. Bestemmelsene etter disse punktene - sammen med andre gjeldende krav og normer – skal bidra til forhindre og motvirke at det oppstår feil og havariere som følge av disse og liknede uønskede hendelser.

Vi forutsetter at regler i henholdsvis *FEF* med veiledning, normer utgitt av NEK (Norsk Elektroteknisk Komité) og REN (Rasjonell Elektrisk Nettvirksomhet AS), følges så langt de er relevante og tilstrekkelige for å oppfylle forskriftens formål og bestemmelser.

Vi vil særlig peke på de ”Nasjonale Normative Forhold (NNA) for Norge” som er utarbeidet av NEK basert på EN og som er tatt inn i NEK 445 (siste utgave). Disse bør følges.

I vurderingene og tiltakene som skal gjennomføres, må det tas hensyn til at klimabelastningene kan øke betydelig i årene som kommer. Videre skal det fullt ut tas hensyn til ulike kombinerte belastninger som følge av for eksempel vind og ising.

5.IX.5 Trasevalg og krav til trasé

Ved planlegging av nye anlegg bør det vektlegges å finne traseer og løsninger som ikke gir risiko for skader og havari som følge av ras/skred, flom, kollisjoner e.l. Dersom ledningen må passere utsatte områder (for eksempel der det er fare for ras og skred) bør parallelle master unngås, om det ikke kan gjøres tiltak som ekstra forstreknings, skredavvisere og liknende.

5.IX.6 Master, oppheng, ledere og liknende

Forskriftens krav oppfylles ikke dersom man anvender svake/mindre stabile konstruksjoner. Slike konstruksjoner kan for eksempel være høyspentmaster med kun én bærende trestolpe i områder med krevende klima eller som hjørnestolper. Unntak gjelder for midlertidige reparasjoner eller spesialkonstruerte reservemaster.

Av hensyn til blant annet estetikk og plass har flere land utviklet og dels tatt i bruk ukonvensjonelle stålmaster og liknende for høyere spenninger. Før slike eventuelt tas i bruk i Norge i større omfang, bør det både ut fra teoretiske beregninger og praktisk erfaringer, kunne dokumenteres at disse tåler de belastningene de kan bli utsatt for i Norge. For øvrig viser vi til veiledningen til *FEF* kapittel 6 Høyspenningsluftlinjer.

5.IX.7 Elektrisk og mekanisk dimensjonering

Kraftledningen skal til enhver tid tåle den spenningen og den overføringsevnen som er gitt i konsesjonen og er innrapportert til og vedtatt av systemansvarlig (eventuelt NVE) etter bestemmelser om overføringsgrenser i *forskrift om systemansvaret i kraftsystemet (FoS)*.

For krav til isolasjon med videre for luftledning, se veiledningen til *FEF* kapittel 4 Høyspenningsluftlinjer.

Kraftledningen skal tåle de påregnelige mekaniske påkjenningene den kan bli utsatt for. Som generell norm for dimensjonering av kraftledninger legges til grunn en returtid for klimabelastninger og andre påkjenninger på 150 år ut fra de lokale forholdene. Selskapet kan for en gitt ledningstrekning differensiere dimensjoneringen og velge den beste løsningen ut fra stedlige forhold. Selskapet må innhente de nødvendige opplysningene og ha tilgang til nødvendig kompetanse for å gjennomføre dette på forsvarlig vis.

For kraftledning i klasse 3 må lengre returtid som 500 år vurderes. Med returtid forstås her samme begrep som definert i veiledning til *FEF*. Videre må høye krav til kombinerte laster (for eksempel vind og ising) vurderes.

Det skal tas særlige hensyn til utsatte områder for belastninger som her er nevnt, forsyningsområdets samfunnsmessige betydning, og om området er uten alternativ forsyning (radialer og liknende).

5.IX.8 Kontroll og vedlikehold

Det skal føres jevnlig (minst én gang i året) kontroll både med selve ledningen (jf. linjebefaring), traséen og dens omgivelser. Kontrollen må også gjelde avstand til vegetasjon (luftledning), manglende overdekning og beskyttelse (kabel) og gjenstander og forhold som kan representere en risiko for ledningens drift eller tilstand. Kontroll skal også foretas når ledningen har vært utsatt for unormalt stor påkjenninger.

Kontrollen skal avdekke om den ledningstekniske, elektriske og mekaniske tilstanden er tilfredsstillende. Dette gjelder også råde, korrosjon, skader og annet som kan svekke ledningens mekaniske konstruksjon og tåleevne.

For metoder og hyppighet for blant annet skogrydding, se avsnitt om Særlig krav til analyse nedenfor.

Det gjelder kontroll med ledningens elektriske føringsvei ved hjelp av målinger, detaljbilder, termovisjonsfotografering og toppbefaringer. Ved toppbefaring må det tas regelmessige stikkprøver av utsatte punkter som opphengsklemmer og skjøter - særlig på værharde strekninger.

Det skal føres kontroll med at ikke ledningen har vært utsatt for belastninger som over tid kan være større enn dens tåleevne. For eksempel skjevtrukne stolper/ master, slakke barduner, bøyde stag eller avstivninger, sprekker og krakeleringer i stolper og fester.

Kritiske forhold som avdekkes etter dette punktet, skal utbedres uten ugrunnet opphold, øvrige forhold etter en lokal vurdering innen rimelig tid.

5.IX.9 Reparasjonsberedskap, krav til reservedeler, utstyr og kompetanse.

Der ledningen må legges over eller passere værharde eller andre utsatte eller lite tilgjengelige områder, må den totale reparasjonskapasiteten tilpasses dette. Se for øvrig veiledning til kapittel 4 Ressurser og reparasjonsberedskap.

5.IX.10 Særlig om lange fjordspenn

For lange fjordspenn bør man vurdere å etablere en ekstra faseline slik at kursen kan fungere i tilfelle havari og liknende. Alternativt skal det være tilgang på særskilt

reparasjonsberedskap, med nødvendig utstyr og reserve spesialliner. Se også veiledning til kapittel 4 Ressurser og reparasjonsberedskap.

NVE viser for øvrig til Luftfartstilsynets forskrifter om merking av luftfartshinder.

5.IX.11 Særlig om sjøkabel med kabelanlegg

Minst hvert tiende år bør kabler og kabeltraséer i klasse 2 og 3 kontrolleres ved hjelp av ROV (Remotely Operated Vehicle) eller liknende for å kontrollere overdekking eller andre forhold som kan utgjøre en risiko for kabelen, og så langt mulig kabelens tilstand for øvrig. Dette gjelder særlig i skvalpesonen og andre utsatte steder hvor kabelen ligger ubeskyttet, eller kan være utsatt for uønskede virkninger av skipsfart, oppankring, fiske og annen maritim virksomhet.

For å overvåke tilstanden i klasse 2 og 3 oljekabler bør det etter kabelens konstruksjon og virkemåte anordnes hensiktsmessig instrumentering for blant annet å overvåke oljetrykk og temperatur.

Muffeanlegg og liknende har samme klasse som den ledningen eller stasjonen de er en del av. Se for øvrig veiledning til kapittel 4 Ressurser og reparasjonsberedskap.

5.IX.12 Særlige krav til analyse

Overnevnte forhold skal så langt det er relevant vurderes i en risiko- og sårbarhetsanalyse for ledninger.

Fra NVE-rapporten *Trær til besvær* (nr 45-2012) gis følgende anbefaling for ROS-analyser knyttet til skogrydding spesielt for tiltak utenfor klausulert bredde. Følgende vurderinger kan være et utgangspunkt for en risiko- og sårbarhetsanalyse av nettet:

1. For hvilke linjer er konsekvensene av utfall størst?
 - Viktige kunder, mange kunder, manglende redundans osv. Konsekvensklasser og akseptkriterier.
2. Hvilke linjer er mest utsatt for utfall?
 - Tidligere hendelser, eldre skog, høyde over havet, topografi osv.
3. Hva er kostnadene ved utbedringer av utfall?
 - Tilgang til linjene, type trær som faller på.
4. Hva er kostnadene ved tresikre linjer, sikringshogst og utbedring etter utfall?
 - Kartlegging og analyse.
5. Plan og tiltak

Ut fra en slik analyse kan det lages enkel risikomatrise (sannsynlighet og konsekvens), og nettet kan deles i ulike risikoklasser med ulike grader av ryddetiltak etter risiko. Ut fra dette lages en ryddeplan for hvor det henholdsvis må ryddes og bør ryddes, samt omfanget av ryddingen. Ryddedefrekvens differensieres etter lokal tilvekst.

Del X Fjernvarmesentral mv.

5.X.1 Fjernvarmesentral klasse 1

1.1	<i>For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg gjelder følgende krav:</i>
1.1.1	Det skal etableres en adgangskontrollert sone som omfatter alle adkomster til anlegget. Fysisk sikring skal som et minimum omfatte et solid bygg med dører/ porter, vinduer og øvrige adkomster. Disse skal oppfylle krav til normalt sikringsnivå etter fastsatte normer.
1.1.2	Brannsikring skal oppfylle krav i henhold til andre relevante forskrifter og normal brannmotstand etter fastsatt norm.
1.1.3	Rom for lokal driftskontroll, styring og samband skal være egne adgangskontrollerte soner, og skal oppfylle krav til normalt sikringsnivå og brannmotstand etter fastsatte normer.
1.1.4	For egen stasjonsstrømforsyning skal anlegget ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Et mobilt aggregat må kunne kobles til innenfor batteritiden. Anlegget må samlet sett ha en gangtid på minst ett døgn.
1.1.5	Det skal være tilgang på reserver for viktige komponenter.

5.X.1.1 Generelt om fjernvarmesentraler klasse 1

Fjernvarmesentraler skal sikres som øvrige produksjonsanlegg i klasse 1, så langt disse reglene passer.

5.X.2 Fjernvarmesentral klasse 2

2.6	<i>For fjernvarmeanlegg gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>
2.6.1	Beredskapsmyndigheten kan fastsette særlige krav til sikring av fjernvarmeanlegg.

5.X.2.1 Generelt om fjernvarmesentraler klasse 2

Fjernvarmesentraler i klasse 2 skal sikres minst like godt som fjernvarmesentral i klasse 1. NVE kan vedta ytterligere krav til sikringstiltak og –nivå som enkeltvedtak.

§ 5-7. Vedtak om sikring eller klasse

Beredskapsmyndigheten kan treffe vedtak om andre eller ytterligere sikringstiltak i medhold av energiloven § 9-2 annet, jf tredje ledd. Ved vedtak skal det tas hensyn til anleggets eller systemets betydning for energiforsyningen.

Beredskapsmyndigheten kan treffe vedtak om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av § 5-2 dersom det anses nødvendig.

Beredskapsmyndigheten kan treffe vedtak om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av tidligere vedtak dersom det anses nødvendig.

5.7.1 Hensikten med bestemmelsen

Bestemmelsen gir NVE hjemmel til å treffe vedtak om sikring og klasse basert på andre kriterier og metoder enn de som framgår av §§ 5-2, 5-4, 5-5 og 5-6.

5.7.2 Andre eller ytterligere sikringstiltak

Første ledd gir adgang til å treffe vedtak om andre eller ytterligere sikringstiltak fordi en forskriftsfestet klassifisering og krav til sikringstiltak ikke fullt ut kan ta hensyn til alle forhold som er relevant for beskyttelse av alle aktuelle anlegg. Det er derfor nødvendig å åpne for noen grad av individuell vurdering av et anleggs betydning for energiforsyningen.

5.7.3 Klassifisering etter enkeltvedtak

Annet ledd gir adgang til å treffe vedtak om at et anlegg som ikke er automatisk klassifisert etter § 5-2, likevel skal klassifiseres. Bestemmelsen gir også adgang til å vedta at et anlegg skal plasseres i en annen klasse enn det som ellers ville følge av bestemmelsene i § 5-2 om klassifisering.

5.7.4 Klassifiserte anlegg kan få ny klasse

Tredje ledd gir adgang til å treffe vedtak som innebærer at et anlegg eller system plasseres i en annen klasse enn det som ellers ville følge av tidligere vedtak. Dette omfatter både vedtak truffet etter BfK av 2002 og etter tidligere regelverk.

§ 5-8. Analyse

Virksomhet som planlegger å bygge eller vesentlig endre eller utvide anlegg som er eller vil være klassifisert etter § 5-2, skal på bakgrunn av anleggets klasse etter § 5-2 eller enkeltvedtak, foreta en risiko- og sårbarhetsanalyse og prosjektere, utføre og sikre anlegg og system som angitt i denne forskrift.

5.8.1 Hensikten med bestemmelsen

De foregående bestemmelsene i dette kapitlet fanger i betydelig grad opp de vesentligste risikoer et anlegg kan bli utsatt for og anviser tiltak mot disse. Det vil likevel være lokale forhold med hensyn til omgivelser eller anleggets art som må vurderes særskilt for å få et riktig, fullstendig og balansert hele.

Ifølge § 2-4 om risiko- og sårbarhetsanalyser, skal enheten utarbeide en risiko- og sårbarhetsanalyse (ROS-analyse) for enheten som helhet inkludert anlegg.

Bestemmelsene i § 5-8 er en videreføring av kravene til lokal analyse i § 5-4 i BfK av 2002, men med den endring at anleggenes klasse nå i det vesentlige forskriftfestes.

Dersom man følger forskriftens spesifikke krav, skal normalt grunnsikringen være ivaretatt. Analyse skal utføres både som en kvalitetssikring av grunnsikringen, og for å fange opp lokale forhold (f.eks. ising, flom eller skred) og risikofaktorer som krever supplerende sikringstiltak eller høyere sikringsnivå.

Dette analysekravet gir ikke enheten anledning til å velge løsninger som er svakere enn det grunnsikringsnivået som følger av kravene i denne forskriften. Som det framgår av innledningen til vedleggene til § 5-3 punkt 1 for klasse 1 og punkt 2 for klasse 2 og 3, kan andre løsninger aksepteres dersom det kan dokumenteres at man oppnår et minst like godt sikringsnivå. Risiko- og sårbarhetsanalyser vil være en del av en slik dokumentasjon.

5.8.2 Nærmere om analysen

Analysen skal omfatte alle uønskede hendelser som kan ramme et anlegg i forhold til naturgitt skade, teknisk svikt og tilsiktede ødeleggelser. Analysen skal først og fremst vurdere sårbarhet og uønskede konsekvenser. Fokuset bør være på sikring av ledelse og drift, samt mulig skade på energiforsyningsanlegg. Dette gjelder også driftskontrollsystemer og sambandsanlegg. Enheten må analysere alle uønskede hendelser som kan tenkes å forekomme innenfor ovennevnte kategorier, selv om sannsynligheten kan virke liten.

Som norm for sannsynlighetsskala og konsekvensskala (forsyningssikkerhet) brukes skalaen som angitt i risikomatrisen i NVEs Veiledning i ROS for kraftforsyningen.

I analysen av risiko for bevisste handlinger som inntrengning og skadeverk, skal det tas hensyn til bruk av hjelpemidler med lett (for eksempel vanlig håndverktøy) og middels (tyngre verktøy, kjøretøy) tilgjengelighet. For anlegg i klasse 3 må analysen også dekke mulig bruk av hjelpemidler som i utgangspunktet er lite tilgjengelige.

5.8.3 Planlegge og utføre anlegg og systemer

På grunnlag av kravene i §§ 5-3, 5-4 og 5-6 gjennomføres sikringstiltakene som følger:

- Grunnsikring – med tilpassning til lokale forhold.
- Permanent tilleggssikring.
- Forberedt tilleggssikring.

Alle vurderinger som enheten gjør, samt tiltak enheten iverksetter, skal dokumenteres i henhold til § 2-10 Internkontrollsystem.

§ 5-9. Meldeplikt om sikringstiltak

Virksomheter som planlegger å bygge, endre eller utvide konsesjonspliktige anlegg, skal senest ved søknad om konsesjon sende beredskapsmyndigheten skriftlig melding om hvilken klasse anlegget vil bli bygget etter, jf § 5-2.

For driftskontrollsystemer og annet uten konsesjonsplikt gjelder en tilsvarende plikt om melding i god tid før byggestart.

Melding skal gis elektronisk eller på annen måte som beredskapsmyndigheten bestemmer. Meldingen skal være vedlagt den informasjon som beredskapsmyndigheten bestemmer.

5.9.1 Hensikten med bestemmelsen

Sikringstiltak må planlegges og prosjekteres tidlig i prosessen, slik at sikkerhets- og beredskapshensyn inngår som en del av konsesjonsprosessen på lik linje med andre hensyn. Sikringstiltak kan dermed utføres på en mest mulig hensiktsmessig måte og kostnadene kan reduseres.

5.9.2 Klassifisering skal meldes ved søknad om konsesjon

Som tidligere nevnt under § 5-2 Klasser vil anleggene nå som hovedregel være forskriftsmessig klassifisert, slik at klassen i utgangspunktet er kjent allerede i planleggingsfasen. Ved bygging av nye eller endringer av eksisterende anlegg som

utløser behov for konsesjon etter *energiloven*, skal det vedlegges et skjema (vedlegg 1 til veiledningen) til konsesjonssøknaden. Skjemaet skal innholde en kortfattet bekreftelse på klasse og utførelse av sikringstiltak. Det skal gis en begrunnelse for eventuelle avvik i sikringsnivået.

Dersom kriteriene som er angitt i § 5-2 plasserer anlegget i en klasse som etter konsesjonssøkers vurdering avviker vesentlig fra anleggets reelle beredskapsmessige betydning, kan det søkes om å få endret klasse. Slik søknad skal være beredskapsmessig begrunnet, kort og konsis med relevante vurderinger ut fra forskriftens hensyn og bestemmelser.

NVE vil vurdere om søknaden er tilstrekkelig begrunnet, og kan eventuelt fatte vedtak om annen klasse og sikringstiltak etter § 5-7. NVE vil om nødvendig be om tilleggsopplysninger.

5.9.3 Driftskontrollsystemer meldes før byggestart

Driftskontrollsystemer omfattes ikke av konsesjonsplikt. For disse er derfor fortsatt nødvendig med meldeplikt som en videreføring av den eksisterende ordningen. Særlig gjelder dette driftskontrollsystemer i klasse 2 og 3, hvor det fattes enkeltvedtak om klasse på grunnlag av de opplysninger NVE mottar gjennom slik melding. Melding skal som i dag kun sendes NVE dersom det er så store endringer i driftskontrollsystemets funksjon at det kan påvirke anlegget klasse, eller ved store fysiske ombygginger og strukturelle endringer som en bekreftelse på at anlegget blir prosjektert og utført i henhold til forskriftens bestemmelser for vedkommende klasse.

5.9.4 Om form på melding

Tredje ledd fastsetter at det er beredskapsmyndigheten som fastsetter hvordan slik melding skal gis og hvilke opplysninger den skal inneholde. Det vises her til ovennevnte.

Skjema for konsesjonspliktige anlegg – vedlegg 1 til veiledningen.

Skjema for driftskontrollsystemer – vedlegg 2 til veiledningen.

Når det gjelder innsending av informasjon, vil NVE peke på at informasjonssikkerheten etter forskriftens kapittel 6 om informasjonssikkerhet skal ivaretas, vurdert etter innholdets art og grad av sensitivitet. Disse skjemaene er merket **”Underlagt taushetsplikt etter energiloven § 9-3 jf bfe § 6-2. Unntatt fra innsyn etter offentleglova § 13”**. Skjema som sendes til NVE sammen med søknad om konsesjon, og skal være et eget separat vedlegg til konsesjonssøknaden.

§ 5-10. Vakthold

Eier eller driver av kraftforsyningsanlegg som er prioritert for vakthold i ekstraordinære situasjoner, skal bidra til planlegging og gjennomføring av vaktholdet i samarbeid med politi og forsvar.

Plikten omfatter blant annet:

- a. Påvise anleggets vitale deler og beskaffenhetsforøvrige.*
- b. Anskaffe materiell for sikring av anlegget og gjennomføre øvrige tiltak for å hjelpe vaktstyrken.*

c. Tilrettelegge for øvelser på anleggets område.

Beredskapsmyndigheten kan etter denne paragraf gi nærmere bestemmelser for objektsikring og gi bestemmelser for gjennomføring av øvelser i høyspenningsanlegg.

5.10.1 Hensikten med bestemmelsen

Ved ekstraordinære situasjoner som fører til økt beredskap, kan det bli nødvendig å planlegge og etablere ekstra vakthold eller benytte innsatser av væpnede styrker fra politi eller med bistand fra Forsvaret ved en del kraftforsyningsanlegg som av NVE og andre myndigheter er vurdert som særlig viktige eller utsatte.

Kriterier for å velge ut slik anlegg beskrives ikke i denne veiledningen. Vi registrerer at disse forholdene er under revurdering. Ved behov kan NVE gi nærmere informasjon.

5.10.2 Planlegging og gjennomføring

Denne bestemmelsen pålegger eier eller driver av vedkommende prioriterte kraftforsyningsanlegg/ objekt en del plikter, herunder å på vise anleggets vitale deler og beskaffenheter for øvrig.

Ved slik vurdering må enheten legge følgende faktorer til grunn:

- Umiddelbare konsekvenser av skade/ødeleggelse.
- De ulike anleggenes sårbarhet og beskyttelse.
- Reparasjonsmuligheter og erstatningstider.
- Alternativer, muligheter for omlegginger og improvisasjoner.

5.10.3 Tilrettelegge for øvelser m.m. ved høyspenningsanlegg

Eier eller driver skal tilrettelegge for øvelser m.m. ved høyspenningsanlegg. NVE har i samarbeid med DSB (jf. Eltilsynet) fastsatt et eget øvingsdirektiv: *Direktiv for øvelser ved m.m. ved kraftforsyningsanlegg* på www.nve.no. Dette gir de ulike parter ved slike øvelser klare plikter og rettigheter og legges til grunn ved alle øvelser i forbindelse med høyspenningsanlegg.

5.10.4 Adgang for politi og forsvar

Energiloven gir etter endringen vedtatt i 2012 ”adgang for politiet og militære myndigheter når dette har sammenheng med forberedelse til og gjennomføring av væpnet sikring” til grunn, bygg og anlegg. På grunn av at ferdsel i høyspenningsanlegg utgjør en betydelig personrisiko – jf § 9. Adgang i forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg (DSB 2006), forutsetter NVE at nåværende regulering av øvingsvirksomhet og lignende videreføres med en klar fordeling av ansvar og plikter.

§ 5-11. Besøksrestriksjoner

Alle driftssentraler i klassifiserte driftskontrollsystemer, og alle energianlegg klassifisert i klasse 3, skal ha besøksrestriksjoner. Beredskapsmyndigheten kan vedta at også energianlegg i klasse 2 skal ha besøksrestriksjoner.

Ved anlegg underlagt besøksrestriksjoner skal:

a. De besøkende følge en fast avgrenset rute.

b. De besøkende til enhver tid være ledsaget av en erfaren og ansvarlig representant for anlegget.

c. Det ikke gis opplysninger om sensitiv informasjon etter § 6-2.

e. Fotografering være forbudt med mindre spesiell tillatelse er innhentet fra ansvarlig representant for anlegget.

Driftssentraler i klasse 3 skal ha besøksforbud. Beredskapsmyndigheten kan vedta besøksforbud for andre energianlegg i klasse 3.

5.11.1 Hensikten med bestemmelsen

Bestemmelsene skal blant annet forebygge, forhindre uønsket informasjonsinnhentning, plassering av uvedkommende gjenstander (bomber, spionutstyr o.l.), sabotasje, trusler og vold mot ledelse og personell, eller utrettmessig inngripen eller overtakelse.

De er i det vesentlige en videreføring av § 4-6 om besøksrestriksjoner i BfK fra 2002. I tillegg er det innført besøksforbud ved driftssentraler i klasse 3.

Bestemmelsen regulerer besøk og omvisning av for eksempel turister, skoleklasse, foreninger, medier og andre utenforstående. Den er ikke til hinder for den adgang som må finne sted ut fra tjenstlige behov. Den er heller ikke til hinder for besøk av vedkommende selskaps inviterte gjester som selskapet selv kan gå god for. Reglene er de samme for norske og utenlandske statsborgere. Det er nå opp til vedkommende selskap selv å vise den nødvendige varsomhet.

5.11.2 Kontroll med besøk

For å motvirke tilsiktede uønskede hendelser og handlinger eller forberedelser til slike, skal følgende viktige energiforsyningsanlegg ha besøksrestriksjoner:

- Alle anlegg i klasse 3, så langt slikt anlegg har et avlåst eller kontrollerbart område (for kraftledning vil dette være for eksempel muffehus eller kabelkulvert).
- Anlegg i klasse 2 hvor NVE har fattet enkeltvedtak.
- Alle klassifiserte driftssentraler (inklusive relevante IT- og sambandsanlegg, for klasse 3 har besøksforbud).

Ved ovennevnte anlegg kan eier eller ansvarlig driftsselskap ha kortvarige kontrollerte besøk. Det skal i så fall foreligge et informasjonsfaglige bergrunnet behov og være utarbeidet et forsvarlig opplegg for besøket. Ukontrollerte eller tilfeldige turistbesøk uten slikt organisert opplegg, er ikke tillatt.

5.11.3 Besøkets begrensninger

Besøket skal følge en fast avgrenset rute og til enhver tid være ledsaget av en ansvarlig representant for anleggets eier. Ledsagere må kjenne anlegget, beredskapsforskriftens krav, lokal instruks for besøk, og kunne påse at disse og andre krav til sikkerhet blir overholdt.

For at ledsageren til enhver tid skal ha nødvendig oversikt over de besøkende, bør besøket avgrenses både i antall, tid og rom. Antallet besøkende bør begrenses til det antallet

ledsageren til enhver tid kan ha oppsyn med. Normalt bør det ikke være større grupper enn 15 (maksimalt 30) personer, og tiden bør avgrenses til maksimalt to timer.

Ruten bør være avgrenset til de delene av anlegget hvor ledsageren lett kan føre kontroll med besøkende, og hvor det er lite sensitiv informasjon. Om nødvendig avmerkes/separerer tillatt og ikke tillatt område.

Enheten bør unngå kjøring i anlegget. Dersom kjøring er nødvendig, skal dette fortrinnsvis skje med eiers egne kjøretøyer. Det er ikke tillatt å la ukjente kjøretøyer kjøre i anlegget.

NVE forutsetter at DSBs krav til brannsikkerhet og sikkerhet i elektriske anlegg følges.

5.11.4 Identifikasjon og besøkslister

For å hindre at uvedkommende får adgang og for å ivareta personsikkerheten, må alle besøkende identifiseres. Dette skjer ved framvisning og kontroll av godkjent og gyldig identifikasjon med bilde, navn, nasjonalitet, fødselsdato og underskrift (førerkort eller bankkort). For utenlandske statsborgere utenfor Norden vil dette bety pass eller EU-godkjent identifikasjon (såkalt Nasjonale identitetskort). Personer uten identifikasjonspapirer kan ikke gis adgang. Unntak kan gjøres for eksempel ved besøk av en lokal skoleklasse eller andre velkjente personer som eier kan gå god for.

Før besøket i anlegget skal det settes opp en liste (besøksprotokoll) med alle de besøkendes navn, nasjonalitet og fødselsdato. Denne bør oppbevares i minimum 5 år etter besøket.

5.11.5 Sensitiv informasjon

Under besøket skal ikke enheten spre sensitiv informasjon, se også §§ 6-1 og 6-2 om sensitiv informasjon. Enheten kan ikke gi detaljerte opplysninger om anleggets oppbygning, drift eller lignende forhold.

5.11.6 Forbud mot fotografering og medbringning av gjenstander

Fotografering er forbudt, med mindre spesiell tillatelse er innhentet fra ansvarlig representant for anleggets eier og det er tatt hensyn til sikkerhetsmessige forhold. Det kan for eksempel gis anledning til å ta et oversiktbilde av generatorhallen fra et utpekt sted.

Det er ikke tillatt å ta med større eller uvanlige gjenstander inn i anleggets sentrale og vitale deler, også av risiko for eksempelvis medbrakte eksplosiver, jamme- eller avlyttingsutstyr.

5.11.7 Instruks for besøk

Instruks for besøk bør minst omfatte følgende:

- Kravene som stilles i denne bestemmelsen.
- Begrensninger beskrevet i veiledningen til dette kapittelet.
- Kravene i beredskapsforskriften for øvrig.
- Forhold som kommer fram av ROS-analysene.

5.11.8 KBO-enhetens inviterte gjester

Det kan være aktuelt for eier å invitere besøkende med et faglig rettmessig informasjonsbehov, eksempelvis bransjefolk, kunder og samarbeidende etater. Dersom dette er personer KBO-enheten kjenner og kan gå god for, kan enheten gjøre unntak fra ovennevnte begrensninger, men enheten må da utvise sikkerhetsmessig aktsomhet.

5.11.9 Studie- og andre liknende opphold

Ved studie- og andre liknende opphold er det en forutsetning at anleggets eier/ driftsansvarlig legger til rette for, og har tett oppfølging av alle sikkerhetsforhold. Det kan ikke gis selvstendig eller ukontrollert adgang til anlegget eller anleggets IKT- systemer. Dersom studenter utfører oppdrag eller tjenester, gjelder også de andre bestemmelsene i kapittel 6.

5.11.10 Besøksforbud ved driftssentraler i klasse 3

Av hensyn til informasjonssikkerhet og økt vekt på IKT-sikkerhet, særlig for driftskontroll, er det vedtatt at driftssentraler i klasse 3 skal ha besøksforbud.

5.11.10.1 Hvem forbudet gjelder for

Besøksforbudet gjelder for de gruppene som denne paragrafen omfatter. Besøksforbudet gjelder ikke tjenstlig begrunnede behov eller vedkommende selskaps egne inviterte gjester som selskapet selv kan gå god for. Det siste kan omfatte representanter fra andre enheter i KBO, samarbeidende organisasjoner/ etater og viktige kunder når det foreligger et reelt informasjonsbehov. Men også her skal det utvises sikkerhetsmessig aktsomhet, identitet skal kontrolleres og besøket protokolleres. Fotografering og liknende er ikke tillatt.

For mediene og liknende er forbudet absolutt. Eventuell informasjonsvirksomhet og mottak av presse kan ivaretas med for eksempel et besøksrom adskilt fra selve driftssentralen.

5.11.10.2 Hvor det er forbud

Driftssentral hvor besøksforbudet gjelder/ omfatter følgende (jf adgangskontrollert sone § 5-1):

- Funksjonelt hvor man kan utøve driftskontroll (kontrollrom, beredskapsrom og teknisk rom med terminaltilkobling).
- Systemtekniske rom som understøtter driftskontrollfunksjoner/–system (prosessmaskiner, samband, nødstrøm mv.).
- Øvrige fysisk rom/områder som skal være egne/egne adgangskontrollerte sone(r) etter vedlegg 2 til bfe, punkt 2.4.1.2 og vedlegg 3 til bfe, punkt 3.4.1.3.

5.11.11 Besøksforbud ved andre anlegg

Besøksforbud kan også vedtas for andre viktige anlegg.

Kapittel 6. Informasjonssikkerhet

Kapittel seks utdyper *energiloven* § 9-3, og konkretiserer hvordan plikten til å beskytte sensitiv informasjon om energiforsyningen kan etterleves av KBO-enhetene. Samtidig gjelder plikten til å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen. Plikten gjelder for *enhver*, det vil si ikke bare begrenset til KBO-enhetene. Tilsyn og erfaring har vist at det er et behov for å synliggjøre hva sensitiv informasjon er, hvem som er rettmessige brukere og hvordan slik informasjon skal håndteres.

Energiloven § 9-3 lyder:

”Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor denne befinner seg og hvem som har tilgang til den. Det skal etableres avskjerming og beskyttelse av sensitiv informasjon.

Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.

Departementet kan gi nærmere forskrifter om informasjonssikkerhet i kraftforsyningen og om taushetsplikten.”

Nærmere om ”enhver”

Etter *energiloven* § 9-3 annet ledd gjelder taushetsplikten for enhver. Det vil si for alle som tilfeldigvis kommer i kontakt med taushetsbelagt informasjon. Plikten gjelder både for fysiske og juridiske personer uansett hvordan disse er organisert. I forarbeidene er det uttrykkelig sagt at taushetsplikten ikke er begrenset til KBO-enheter. Det er også forklart at ”Med enhver menes alle som kommer i kontakt med sensitiv informasjon om kraftforsyningen, for eksempel netteiere, kontraktører og tilsynsmyndigheter.”

Selv om taushetsplikten gjelder for enhver, mener vi at det er grunn til å skille mellom KBO-enheter og andre (enten det er offentlige myndigheter, medier eller privatpersoner). I forarbeidene til beredskapsforskriften er det understreket at det er den enkelte KBO-enheten som er eier av den sensitive informasjonen som også har ansvaret for at informasjonen ivaretas på forskriftsmessig måte, også når den formidles videre til andre som har tjenstlig behov.

Ingen tidsmessig grense for taushetsplikt

Det er ikke satt noen tidsmessig grense for hvor lenge taushetsplikten gjelder. Taushetsplikten gjelder derfor så lenge informasjonen er sensitiv. Plikten gjelder både under arbeid og i fritiden. Dersom man har fått kjennskap til den sensitive informasjonen i forbindelse med egen stilling, gjelder den også etter at man eventuelt har sluttet i stillingen.

Hva taushetsplikt innebærer

Taushetsplikten innebærer enkelt sagt at man skal passe på og sikre den sensitive informasjonen slik at det bare er rettmessige brukere som får tilgang til den. Alle som har taushetsplikt, har derfor ikke taushetsplikt overfor alle andre. Regelverket bygger på at

det er KBO-enhetene som i utgangspunktet er eiere av den kraftsensitive informasjonen og har ansvar for å vurdere hvem som er rettmessige brukere. Dette følger av *energiloven* § 9-3 første ledd: "Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge ... og hvem som har tilgang til den. ..." Videre er det fastsatt i bfe § 6-1 tredje ledd: "Med rettmessig bruker menes fysiske eller juridiske personer som har tjenstlig behov for sensitiv informasjon". Den enkelte KBO-enheten skal selv avgjøre hvem som har tjenstlig behov for sensitiv informasjon innenfor sin virksomhet og kan avgjøre om det er tjenstlig behov for å videreformidle sensitiv informasjon fra virksomheten til andre utenfor egen virksomhet. Ved vurdering av tjenstlig behov skal det med andre ord tas utgangspunkt i behovet den enkelte KBO-enheten har for å dele informasjonen.

Beredskapsmyndigheten kan i tvilstilfeller avgjøre hvem som er rettmessig bruker. I forarbeidene til § 9-3 står det: "Rettmessige brukere vil primært være selskapets egne ansatte, innleide leverandører og myndigheter med tilsynsansvar på området."

Videre skal man sikre den sensitive informasjonen. Dette gjøres både ved at man faktisk gjør vurderinger av blant annet hva som er taushetsbelagt og at man aktivt hindrer at de som ikke er rettmessige brukere, får "adgang eller kjennskap til informasjonen ved tre typer tiltak: tilgangskontroll, avskjerming og beskyttelse.

De nødvendige vurderingene omfatter etter *energiloven* 9-3 første ledd: "Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den." Bfe § 6-1 første og annet ledd utdyper dette: "Alle KBO-enheter skal etter *energiloven* § 9-3 første ledd identifisere hva som er sensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den".

Å hindre at sensitiv informasjon blir kjent for uvedkommende gjennom tilgangskontroll, betyr at man skal identifisere hvem som er rettmessige brukere og sørge for at denne vurderingen er oppdatert til enhver tid. Avskjerming betyr tiltak i form av merking, oppbevaring, bruk og distribusjon, tilintetgjøring av sensitiv informasjon, jf bfe § 6-3 annet ledd. Beskyttelse betyr tiltak mot avlytting og manipulering fra uvedkommende, samt tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten, jf bfe § 6-3.

§ 6-1. Identifisering av sensitiv informasjon og rettmessige brukere

Alle KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er sensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den.

Identifiseringen av hva som er sensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.

Med rettmessig bruker menes fysiske eller juridiske personer som har tjenstlig behov for sensitiv informasjon. Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for sensitiv informasjon innenfor sin virksomhet og kan avgjøre om det er tjenstlig behov for å videreformidle sensitiv informasjon fra virksomheten til andre

utenfor egen virksomhet. Beredskapsmyndigheten kan i tilfeller avgjøre hvem som er rettmessig bruker.

6.1.1 Hensikten med bestemmelsen

Hensikten med § 6-1 er at enheten skal identifisere hvilken informasjon som kan brukes til å skade energiforsyningen. Enheten skal ha systemer som sørger for at denne typen informasjon oppbevares på riktig måte og at den kun deles med dem som har tjenstlig behov. Kravet skal sette KBO-enheten i stand til å holde oversikt over og kontrollere tilgangen til sensitiv informasjon. Enheten skal oppdage og håndtere brudd på og trusler mot informasjonssikkerheten på en rask og effektiv måte.

6.1.2 Nærmere om identifisering av sensitiv informasjon

KBO-enhetene har etter denne bestemmelsen plikt til å identifisere hva som er sensitiv informasjon. Dette innebærer at KBO-enhetene både må identifisere hvilken informasjon de eier, oppbevarer, produserer med videre som vil være sensitiv etter bokstav a – j i § 6-2. Det forventes også at de gjør en selvstendig vurdering av hvilken informasjon som er så *spesifikk* eller som gir så *inngående kjennskap* om energiforsyningen at den kan brukes av uvedkommende til å *skade anlegg* eller *påvirke funksjoner som har betydning for energiforsyningen*.

6.1.3 Nærmere om oppbevaring av sensitiv informasjon

Sensitiv informasjon om energiforsyningen kan lagres på flere ulike måter. Målet er at KBO-enhetene skal håndtere all sensitiv informasjon i henhold til egen sikkerhetsinstruks (jf § 6-4) uavhengig av hvordan informasjonen er lagret.

Som ledd i dette arbeidet er det viktig at alle KBO-enhetene foretar en helhetlig vurdering av sikkerheten ved oppbevaring og behandling av all informasjon om energiforsyningen. Bestemmelsen er utformet slik at den omfatter alle måter sensitiv informasjon kan oppbevares på. Med formuleringen ”lagring på annen måte” understrekes det at oppbevaring på papir og lagring i elektronisk form ikke er en uttømmende liste.

KBO-enhetene skal også til enhver tid vite hvor den sensitive informasjonen befinner seg. Det betyr at de eksempelvis både skal holde oversikt over hvor informasjon på papir (fysisk) er oppbevart og hvor elektronisk materiale befinner seg (hvilken server med videre).

6.1.4 Nærmere om rettmessig bruker og tjenstlig behov

Rettmessige brukere er definert i § 6-1 tredje ledd, og vil primært være selskapets egne ansatte, innleide leverandører og myndigheter med tilsynsansvar på området. I forarbeidene til forskriften legges det til grunn at det i plikten til å identifisere hvem som har tilgang til slik informasjon, også ligger en vurdering av hvordan den er sikret mot uvedkommende, altså fysiske og juridiske personer som ikke skal ha tilgang til denne informasjonen.

Kravet til beskyttelse av informasjonen innebærer krav til at den ikke skal offentliggjøres for allmennheten, for eksempel gjennom publisering på internett. Kraftsensitiv informasjon skal imidlertid ikke beskyttes på en slik måte at det er til hinder for å dele informasjon når det foreligger et tjenstlig behov. For eksempel vil en kommune kunne ha behov for kraftsensitiv informasjon i egenskap av planmyndighet.

Hver enkelt KBO-enhet må selv vurdere hvem som har et tjenstlig behov for sensitiv informasjon. Dersom det oppstår tvil om hvem som er rettmessig bruker med tjenstlig behov, kan NVE avgjøre om et slikt behov foreligger. Dette innebærer at KBO-enhetene kan kontakte NVE for å få en vurdering av eventuelle tvilstilfeller. Det forutsettes imidlertid at KBO-enhetene har satt seg inn i regelverket, og at virksomhetene i de fleste tilfellene selv kan avgjøre hvem som kan få tilgang, og inngår de nødvendige avtalene om taushetsplikt og beskyttelse av informasjonen (jf § 6-5) i forbindelse med slik informasjonsdeling. Det kan også oppstå tvil når det for eksempel er uklart hvem som er den rettmessig eieren av informasjonen, for eksempel når det dreier seg om informasjon som involverer flere KBO-enheter.

NVE legger til grunn at det i plikten til å identifisere hvem som har tilgang til slik informasjon, også ligger en plikt til å vurdere hvordan den er sikret mot at uvedkommende ikke skal ha tilgang til denne informasjonen, jf § 6-3. Se også merknader til kapittel 7, om beskyttelse av driftskontrollen.

Dersom det foreligger et tjenstlig behov, skal deling av sensitiv informasjon skje på en forsvarlig måte, jf §§ 6-2, 6-4, 6-5 og 6-6.

6.1.5 Om bruk av skytjenester

I de senere årene har bruk av såkalte skytjenester økt betydelig både i norske og internasjonale virksomheter. Skytjenester tillater brukere å leie tilgang til programvare og maskinvare samt lagringsplass for dokumenter eller andre typer filer som drives av en tjenesteyter og er lokalisert på et annet geografisk sted. Lokaliseringen er gjerne et annet land.

Definisjon av skytjenester

Det finnes flere definisjoner og inndelinger av skytjenester, men den vanligste er å dele dem inn i tre:

Software as a Service (SaaS): Dette omfatter applikasjonstjenester som for eksempel tilgang til mail, og tilbys gjennom en tynnklient som nettleser eller en app.

Platform as a Service (PaaS): Kunden tilbys en plattform hvor man kan laste opp eller lage sine egne applikasjoner. Kunden har ikke kontroll over operativsystem og infrastruktur, men har kontroll over applikasjonene som benyttes.

Infrastructure as a Service (IaaS): Kunden kan få tilgang til regnekraft, lagringsplass, nettverk og annen infrastruktur som brukeren kan kjøre programvare på. Kunden kan ha kontroll over eget operativsystem og programvare.

Beredskapsforskriften setter konkrete krav til hva slags informasjon som må skjermes. I § 7-6 Kontroll ved endringer i driftskontrollsystemet er det et forbud mot å benytte skytjenester eller andre eksterne tjenester eller leverandører for overvåking og styring av anlegg i energiforsyningen.

For annen sensitiv informasjon setter denne bestemmelsen begrensninger for bruken av skytjenester, i tillegg til:

- §§ 6-2, 6-3, 6-4 og 6-8 i kapittel 6.

- §§ 7-6 og 7-10 i kapittel 7.

Ønsker man likevel å vurdere bruk av skytjenester må virksomheten gjøre følgende:

- Virksomheten må gjøre en grundig vurdering av hva slags informasjon som skal legges over i skyen.
- Foreta en risikovurdering der man for eksempel vurderer tap av informasjon, eller at den er utilgjengelig av en eller annen årsak.
- Virksomheten må vurdere sikkerhetsnivået på skytjenesten – er den tilstrekkelig slik at man sikrer at kun de som skal ha tilgang på informasjon får tilgang?
- Dersom energisensitiv informasjon skal lagres – kan det dokumenteres at man lagrer informasjonen fysisk i Norge?
- Kan leverandøren garantere at de har sikkerhetsmekanismer (både interne og eksterne) som sikrer at uvedkommende ikke får tilgang til å lese dokumentene?
- Gjennom avtalene med leverandørene må KBO-enheten sikre seg adgang til å foreta inspeksjoner av lokalitetene der informasjonen lagres, for eksempel datahall.
- Sikkerhetsavtaler må utarbeides med leverandøren.
- Avtaler med leverandører skal sikre at NVE har rett til å føre tilsyn med etterlevelse av bestemmelsene om informasjonssikkerhet, jf § 6-5 Anskaffelser i Energiforsyningen.

I sum krever dette følgende kompetanse hos virksomheten;

- Juridisk kompetanse for å holde kontroll med lovkrav og kontrakter.
- Teknisk kompetanse for å analysere og forstå sikkerhetsmekanismer som systemet krever, samt iverksette løsningen.
- Virksomhetsforståelse for å vurdere hvorvidt et nytt system eller tjeneste understøtter bedriftens behov.
- Kommunikasjonskompetanse for å informere og lære opp virksomhetens personell.
- Kompetent prosjektledelse for å sikre at alle de overnevnte forholdene blir ivaretatt og sørge for tverrfaglig risikoanalyse og framdrift.

§ 6-2. Sensitiv informasjon

Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.

Med sensitiv informasjon menes spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen, herunder:

- a. Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband.*

- b. Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg.*
- c. Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.*
- d. Oversikt over fordelingsnett til samfunnsskrittiske funksjoner.*
- e. Nøyaktig kartfesting av jordkabler.*
- f. Forebyggende sikkerhetstiltak mot bevisst skadeverk.*
- g. Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.*
- h. Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.*
- i. Beredskapsplaner for å håndtere bevisst skadeverk.*
- j. Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk.*

6.2.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å klargjøre hva som er sensitiv informasjon om energiforsyningen, og som derfor er underlagt taushetsplikt.

6.2.3 Presisering av hva som er sensitiv informasjon

Det er kun informasjon som er så *spesifikk* eller som gir så *inngående kjennskap* til energiforsyningen, at den kan brukes av uvedkommende til å *skade anlegg* eller *påvirke funksjoner som har betydning for energiforsyningen*, som anses som sensitiv informasjon.

Hva som finnes av sensitiv informasjon om energiforsyningen, vil variere. Det vil bero på en konkret vurdering av hvilken informasjon som må anses som sensitiv. Også sammenstilling av informasjon som ellers ikke regnes som sensitiv, kan gi så spesifikk eller inngående kjennskap at den kan brukes til å skade eller påvirke funksjoner på en måte som har betydning for energiforsyningen. Bestemmelsen må i sin helhet ses i sammenheng med § 6-1 som pålegger hver enkelt KBO-enhet å identifisere informasjon som kan brukes til å skade eller hindre energiforsyningen.

Bokstavene a – j beskriver mer detaljert hva som i utgangspunktet er sensitiv informasjon, og er nærmere forklart under.

Bestemmelsen skiller seg fra tilsvarende bestemmelse i BfK fra 2002, som nå er opphevet, i forhold til hvilken informasjon som anses som sensitiv.

Oversikter over sentral- og regionalnettet med påtegnet spenningsnivå vil ikke lenger være ansett som sensitivt. NVE ønsker å tilrettelegge for en bredere offentlig debatt rundt konsesjonssøknader, og vil derfor at informasjon om synlige kraftledninger, spenningsnivåer og transformeringspunkter ikke lenger skal defineres som kraftsensitiv informasjon. Jordkabler vil fortsatt være definert som kraftsensitiv informasjon, jf bokstav e.

6.2.4 Nærmere om taushetsplikten

Reglene om informasjonssikkerhet er taushetspliktregler, og innebærer at enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen. Rettmessige brukere vil primært være selskapets egne ansatte, innleide leverandører og myndigheter med tilsynsansvar på området.

Bestemmelsen i første ledd om taushetsplikt for sensitiv informasjon gjelder for enhver, det vil si alle som måtte få tilgang til sensitiv informasjon om energiforsyningen, jf *energiloven* § 9-3.

6.2.5 Bokstav a. Alle systemer som ivaretar viktige driftskontrollfunksjoner, herunder også nødvedlig hjelpeutstyr som samband.

Nærmere beskrivelse av hvilke systemer som ivaretar driftskontrollfunksjoner og krav til disse framgår av kapittel 7. I denne bestemmelsen blir det slått fast at informasjonen om disse systemene betraktes som sensitiv, og skal beskyttes. SRO for fjernvarme er et eksempel på et slikt system.

6.2.6 Bokstav b. Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg.

Enlinjeskjema er som hovedregel underlagt taushetsplikt. Dette er imidlertid ikke tilfelle for enlinjeskjemaer som ikke er av avgjørende betydning for energiforsyningen. Dette gjelder blant annet enlinjeskjema for mindre viktige produksjonsanlegg. Det vil si anlegg som ikke har betydning for verken samfunnskritisk virksomhet eller kraftsystemet for øvrig.

6.2.7 Bokstav c. Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.

Detaljert informasjon om klassifiserte anlegg er sensitiv informasjon. Med detaljert informasjon menes anleggets tekniske egenskaper; effekt, installert ytelse, beskrivelse av sikringstiltak og bygningstegninger.

Større transformatorer har lang reparasjonstid og lang leveringstid. Dette innebærer at informasjon som kan benyttes for å identifisere hvilke transformatorer som kan erstatte hverandre i nettet (reserver), er sensitiv informasjon.

Ved inntegning på kart kan transformatorpunkt tegnes inn med symbol for bygning.

6.2.8 Bokstav d. Oversikt over fordelingsnett til samfunnskritiske funksjoner.

Begrepet samfunnskritiske funksjoner inkluderer både viktige forsvarsanlegg og andre virksomheter med sentral betydning for samfunnets sikkerhet og beredskap. Dette vil for eksempel gjelde skjermingsverdige objekter etter sikkerhetslovgivningen. For øvrig vil det kunne variere over tid hva som vil være samfunnskritisk virksomhet og hvor denne er lokalisert, slik at det uansett må foretas en konkret vurdering i hvert enkelt tilfelle.

For nærmere omtale av samfunnskritiske funksjoner, se veiledning til § 4-1 og § 2-6 (viktige samfunnsfunksjoner).

6.2.9 Bokstav e. Nøyaktig kartfesting av jordkabler.

Nøyaktig kartfesting av jordkabler regnes som sensitivt fordi reparasjonstidene for jordkabler er mer omfattende enn for luftledninger. Ved å skjerme nøyaktig informasjon om jordkabler vil NVE sikre at allment tilgjengelig informasjon om luftledninger ikke nødvendigvis viser hele kraftsystemet.

Kartgrunnlaget for jordkabler er i dag ikke nøyaktig. Offentliggjøring av misvisende kart kan medføre fare for feilgraving, og dermed påføre skade på jordkabler. Entreprenører eller andre som skal grave i et område hvor det ligger jordkabler, vil ha et tjenstlig behov for denne informasjonen, og vil kunne få denne hos KBO-enheten.

Ved inntegning på kart kan jordkabler tegnes inn som rett strek fra punkt a til punkt b.

6.2.10 Bokstav f. Forebyggende sikkerhetstiltak mot bevisst skadeverk.

Forebyggende sikringstiltak mot bevisst skadeverk skal ikke offentliggjøres. Dette omfatter tiltak i forbindelse med bygningsmessige forhold, IKT-systemer, vaktordninger med mer. Dette kan eksempelvis være:

- Informasjon om systemer for oppdagelse og reaksjon.
- Lås- og adgangskontrollsystemer.
- Bygningstekniske tiltak som dører, vinduer, transformatorceller og andre konstruksjoner.
- Tiltak for IKT-sikring, både programvare og maskinvare.
- Oversikt over rutiner for vaktordninger og planer for bemanning av anlegg.
- Oversikt over rutiner for innleid vekterselskap.
- Beredskapsrom

6.2.11 Bokstav g. Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.

En reserve driftsentral vil være et alternativt sted som KBO-enheten kan utøve driftskontrollfunksjonen fra. Hvor denne ligger, skal ikke være offentlig kjent. Dette gjelder uavhengig av om driftskontrollfunksjonen utøves fra et kontrollrom eller om driftskontrollen kan utøves ved hjelp av hjemmevaktordninger. I de tilfellene driftskontroll kan utøves av hjemmevakt, er også alle vaktlister med videre underlagt taushetsplikt.

Med særskilte beredskapsanlegg menes eksempelvis:

- Lager av EMP-sikret IKT-utstyr.
- Mobile sambandskontainere.
- Oversikt over lager med komponenter med spesielt lang leveringstid.

Denne listen er ikke uttømmende. Enheten må selv vurdere hva som er særskilte beredskapsanlegg for ledelse og drift.

6.2.12 Bokstav h. Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.

Dersom analyser av tidligere hendelser og beredskapstiltak gjort for å forebygge tilsvarende hendelser, inneholder informasjon som kan brukes til bevisst å skade energiforsyningen, regnes disse for sensitive.

Denne bestemmelsen er ikke til hinder for at informasjon kan deles med berørte etater som kommuner, politi, brann etc. som har et tjenstlig behov for informasjonen. Informasjonen som deles må sikres i henhold til kravene etter §§ 6-2, 6-4, 6-5 og 6-6 (jf *energiloven* § 9-3).

6.2.13 Bokstav i. Beredskapsplaner for å håndtere bevisst skadeverk.

De planene KBO-enheten har for å hindre og håndtere bevisst skadeverk er sensitiv informasjon. Uvedkommende skal ikke kunne få kjennskap til nøyaktig hvilke konsekvenser ulike typer skadeverk får, og skal heller ikke kunne hindre enhetens håndtering og evne til rask gjenoppretting. Det er viktig å ta hensyn til at dersom naturgitt skade og bevisst skadeverk har samme konsekvens for selskapet, skal beredskapsplanene for å håndtere konsekvensen regnes som sensitive. Det er imidlertid viktig at alt personell som inngår i håndteringen, har god kjennskap til denne delen av planverket.

6.2.14 Bokstav j. Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk.

Kapittel 4 i beredskapsforskriften stiller krav om reparasjonsberedskap hos KBO-enhetene. Selskapets ROS-analyser skal vurdere hvilke samlede oversikter som har betydning for håndtering av bevisst skadeverk.

Bokstav j inkluderer også oversikter over IKT-reservedriftsmateriell, samt nasjonale og regionale oversikter.

6.2.15 Nærmere om merking av dokumenter

Sensitiv informasjon om energiforsyningen er underlagt taushetsplikt og unntatt fra innsyn etter *lov om rett til innsyn i dokumenter i offentlig verksemd (offentleglova)*. Den enkelte KBO-enhet har plikt til å vurdere hva som er sensitiv informasjon, og den skal merkes slik:

Bokmål	Nynorsk
Underlagt taushetsplikt etter energiloven § 9-3 jf bfe § 6-2. Unntatt fra innsyn etter offentleglova § 13.	Underlagd teieplikt etter energiloven § 9-3 jf bfe § 6-2. Unntatt frå innsyn etter offentleglova § 13.

Dersom et dokument er merket med taushetsplikt etter denne paragrafen, indikerer det at det er sensitiv informasjon i dokumentet. Enheten kan offentliggjøre de delene av dokumentet som ikke inneholder sensitiv informasjon.

§ 6-3. Beskyttelse, avskjerming og tilgangskontroll

Alle KBO-enheter skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for sensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.

System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.

Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese sensitiv informasjon.

6.3.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sørge for at informasjon som kan brukes til å skade energiforsyningen, beskyttes på riktig måte slik at den ikke blir kjent for uvedkommende.

6.3.2 Nærmere om hva bestemmelsen omfatter

Tiltak som vurderes for tilgangskontroll og beskyttelse bør omfatte:

- Administrative tiltak.
- Tekniske tiltak.
- Tiltak for bevisstgjøring og opplæring.
- Tiltak for å sikre effektiv tilgangskontroll og beskyttelse.

Administrative rutiner for å sikre at kun rettmessige brukere får tilgang til sensitiv informasjon, som:

- Sikkerhetsinnstruks og taushetserklæringer, jf § 6-4.
- Sikkerhetsavtaler eller klausuler i anskaffelseskontrakter, jf § 6-5.
- Bruk av autorisasjonslister.
- Rutiner ved avslutning og endring av ansettelsesforhold og konsulentoppdrag.
- Rutiner for bruk av bærbare elektroniske produkter, som minnepinner, telefoner, bærbare datamaskiner og liknende.
- Regler for å sende sensitiv informasjon, regler for bruk av henholdsvis e-post, brev og faks.
- Rutiner for avhending av informasjon (fysisk makulering, destruksjon av elektroniske lagringsmedier).

Tekniske rutiner for å skjerme sensitiv informasjon både elektronisk og på papir, som:

- Differensiert brukertilgang på server.
- Regler for passordbeskyttelse (lengde og type passord, tid for bytte av passord og liknende).
- Regler for kryptering.
- Robust systemarkitektur og konfigurasjonsstyring.
- Dokumentasjon av systemer og sikringstiltak.
- Rutiner for oppdatering og vedlikehold av sikkerhetstiltak.
- Merking av dokumenter i arkivet.
- Bruk av sertifiserte produkter, for eksempel etter Common Criteria.
- Rutiner og utstyr for beskyttelse mot ondsinnet programvare.

- Rutiner og utstyr for å oppdage, registrere og forhindre uautoriserte forsøk på inntrengning i kraftsensitive systemer og tilhørende støttesystemer.
- Bruk av inntrengningstester på kritiske systemer for å avdekke sårbarheter.
- Rutiner for logging for å avdekke uautorisert bruk av IKT-systemer. Dette gjelder for tilknytninger mot omverdenen, for eksempel internett og oppringte samband, samt nødvendig logging av intern trafikk. Enheten må kontrollere og sikre loggene, samt dokumentere resultater. Nettverkstrafikk tilkoblet kraftsensitive IT-system bør alltid logges. Se veiledning fra NorSIS om logging.
- Fysisk sikring av informasjon og IKT-systemer, samt skjerming mot innsyn.
- Rutiner for sikkerhetskopiering.
- Kontrollert avhending av informasjon og utstyr.

Hensikten med annet ledd er å pålegge KBO-enheten rutiner som sikrer at sensitiv informasjon beskyttes i alle faser av informasjonens livsløp. Det er innhold og ikke alder som er bestemmende for om informasjon skal identifiseres som sensitiv.

Med mobile enheter i tredje ledd menes smarttelefoner, nettbrett og liknende som kan kobles opp mot virksomhetens nettverk for å lese eller laste ned informasjon som kan være sensitiv, for eksempel e-post. For nærmere veiledning med hensyn til IKT-sikkerhet, se kapittel 7. Oppdaterte anbefalinger med hensyn til IKT-sikkerhet.

6.3.3 Nærmere om informasjonens livsløp

Informasjon om energiforsyningen kan ha lang levetid. Selv om klassifiserte anlegg som transformatorstasjoner og kraftstasjoner kan være bygd for mange år siden, kan informasjonen om anleggenes oppbygging og viktigste komponenter fortsatt være gyldige. KBO-enhetene må påse at slik informasjon ikke havner i arkiv hvor de blir offentlig tilgjengelige. Tilsvarende er det viktig at informasjon som er elektronisk lagret, ikke kan gjenopprettes etter at mobile enheter som PCer, mobiltelefoner og nettbrett avhendes.

§ 6-4. Sikkerhetsinstruks

Alle KBO-enheter skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas, og som beskriver identifiseringen som er foretatt i henhold til § 6-1 og hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og skal stille krav til undertegning av taushetserklæring. Sikkerhetsinstruksen skal også omfatte informasjon om at taushetsplikten medfører at sensitiv informasjon ikke skal offentliggjøres.

6.4.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sikre gode rutiner for håndtering av sensitiv informasjon hos KBO-enhetene.

6.4.2 Nærmere om sikkerhetsinstruksen

Sikkerhetsinstruksen for informasjonssikkerhet er en instruks for håndtering og beskyttelse av viktig og sensitiv informasjon, samt viktige informasjonssystemer i

kraftforsyningen, både teknisk og administrativt. Sikkerhetsinstruksen bør være et resultat av tiltak som er kommet fram i den løpende helhetlige vurderingen av informasjonssikkerheten, se § 6-1, og hvordan kravene skal oppfylles.

Det stilles i annet ledd krav om signering av taushetserklæring. For vurdering av hva som regnes som rettmessige brukere, vises det til § 6-1 tredje ledd.

6.4.3 Nærmere om taushetserklæringen

Sikkerhetsinstruksen skal inneholde informasjon om taushetsplikten etter *energiloven* og beredskapsforskriften, og stille krav om at ansatte og andre rettmessige brukere (av informasjonen) undertegner en taushetserklæring. NVE har utarbeidet en mal for slike taushetserklæringer (se vedlegg 3) som KBO-enheten kan benytte.

§ 6-5. Anskaffelser i energiforsyningen

KBO-enheter som setter ut oppdrag til leverandører og andre med oppdrag for eller i energiforsyningen, skal påse at disse er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. Det skal også i avtale opplyses at beredskapsmyndigheten kan føre tilsyn med etterlevelsen av disse bestemmelsene. Tilsvarende opplysningsplikt gjelder for leverandører når disse inngår kontrakt med underleverandører.

Plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves.

Bestemmelsene i første og annet ledd gjelder tilsvarende når KBO-enheter setter ut oppdrag for prosjektering, installering, vedlikehold og feilretting av driftskontrollsystemet.

6.5.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sikre at kravene til informasjonssikkerhet blir ivaretatt når KBO-enheten setter bort oppdrag der oppdragstaker blir kjent med sensitiv informasjon.

6.5.2 Nærmere om inngåelse av kontrakter

Dersom en leverandør av varer eller tjenester kan bli kjent med kraftsensitiv informasjon, skal kontrakten med leverandøren inneholde opplysninger om informasjonssikkerhet, taushetsplikt og hvordan kravene skal overholdes. Det er KBO-enhetenes ansvar å sikre at kravene til korrekt håndtering av sensitiv informasjon blir ivaretatt av leverandører. For vurdering av hva som er sensitiv informasjon, vises det til §§ 6-1 og 6-2.

Ordningen med landsdekkende sikkerhetsavtaler med leverandører blir avviklet fra og med 01.01.2014. I framtiden vil NVE kun inngå sikkerhetsavtaler med egne leverandører.

Det er tillatt for KBO-enhetene å inngå generelle sikkerhetsavtaler med egne leverandører som det kan henvises til i de enkelte kontraktene som omhandler mer spesifikke leveranser. Et slikt eksempel kan være en kontrakt mellom en KBO-enhet og et konsultentselskap som skal benyttes til flere ulike oppdrag. Det er imidlertid KBO-enheten selv som er ansvarlig for utforming og inngåelse av slike avtaler. NVEs mal for avtaler med egne leverandører (sikkerhetsavtaler) kan benyttes som mal.

6.5.3 Nærmere om ansvar for tilsyn

Plikten til å påse at leverandører beskytter sensitiv informasjon innebærer ikke at KBO-enheten selv er ansvarlig for å føre tilsyn. Dette ansvaret vil fortsatt ligge hos NVE. Bestemmelsen innebærer at beredskapsmyndigheten har rett til å føre tilsyn med håndtering av all sensitiv informasjon leverandører og underleverandører kan komme i kontakt med, basert på kontrakten inngått mellom KBO-enhetene og deres leverandører. Retten til å føre tilsyn omfatter også håndtering av sensitiv informasjon hos leverandører med oppdrag i forbindelse med enhetens driftskontrollsystem.

6.5.4 Nærmere om utveksling av informasjon mellom KBO-enhetene

Samtlige KBO-medlemmer er underlagt både *energiloven* og beredskapsforskriften. Det er derfor ikke påkrevet med sikkerhetsavtaler for utveksling av kraftsensitiv informasjon mellom KBO-enhetene. Utveksling av sensitiv informasjon skal alltid vurderes ut fra tjenestemessige behov.

6.5.5 Nærmere om tilgang til sikkerhetsgradert informasjon

Ved oppdrag som medfører at leverandører kan få tilgang til sikkerhetsgradert informasjon, skal anskaffelsen gjennomføres i samsvar med bestemmelser gitt i medhold av *sikkerhetsloven*.

§ 6-6. Begrenset anbudsinnbydelse

Anbudsinnbydelser og lignende skal begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller sensitiv informasjon om energiforsyningen blir offentlig tilgjengelig gjennom anbudsdokumentene.

Forståelsen av begrenset anbudsinnbydelse bygger på anskaffelsesregelverket.

6.6.1 Hensikten med bestemmelsen

Bestemmelsen skal sørge for at sikkerhetsgradert informasjon eller sensitiv informasjon om energiforsyningen ikke blir kjent gjennom offentliggjøring av anbudsdokumenter.

6.6.2 Nærmere om begrenset anbudsinnbydelse

Begrenset anbudsinnbydelse er i henhold til anskaffelsesregelverket en anskaffelsesprosedyre som tillater at bare leverandører som er invitert av oppdragsgiver til å delta, kan gi tilbud. Med begrepet "anskaffelsesregelverket" sikter NVE til lover og forskrifter for offentlige anskaffelser.

Dersom anbudsdokumentene eller oppdraget inneholder sensitiv informasjon, kan anbudet begrenses ved at kun leverandører som har inngått sikkerhetsavtale med KBO-enheten, får tilsendt anbudsdokumenter.

Andre ledd viser til lover og forskrifter for offentlige anskaffelser. For anskaffelser som innebærer utlevering av sikkerhetsgradert informasjon, vises det til *sikkerhetsloven* med forskrifter. Det vises forøvrig til *forskrift om innkjøp i forsyningssektorene*.

§ 6-7. Personkontroll

Person som vil kunne få tilgang til informasjon som er sikkerhetsgradert etter lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven), skal være

sikkerhetsklarert og autorisert. Autorisasjon for BEGRENSET kan skje uten forutgående sikkerhetsklarering.

6.7 1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sikre at personer som får tilgang til informasjon som er sikkerhetsgradert i henhold til *sikkerhetsloven*, er skikket til å motta slik informasjon, og at de kun mottar sikkerhetsgradert informasjon etter tjenstlig behov.

Ansatte i energiforsyningen kan søke om sikkerhetsklarering begrunnet i tjenstlige behov.

NVE er klareringsmyndighet og foretar sikkerhetsklareringen basert på personkontroll der de innhenter relevante opplysninger til vurdering av personens antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad.

6.7.2 Framgangsmåte

- Enheten må skaffe, og den ansatte må fylle ut, Statens personopplysningsblankett (X-0136/1). Opplysningene som gis på blanketten skal være fullstendige og oppriktige. Utelatelse av opplysninger som er av betydning for vurdering av sikkerhetsmessig skikkethet, vil veie tungt i avgjørelsen om klarering.
- Blanketten undertegnes og legges i egen konvolutt merket PERSONKONTROLL.
- Enheten må lukke konvolutten og sende den sammen med undertegnet taushetserklæring (X-0138), og et følgebrev fra KBO-enheten som begrunner behovet og nødvendig nivå for sikkerhetsklarering. Konvolutten sendes til NVE, Beredskapsseksjonen, Postboks 5091 Majorstua, 0301 OSLO.
- NVE avgjør om personen kan sikkerhetsklareres.
- NVE sender kopi av eventuelt klareringsbevis til beredskapskoordinator. Beviset skal oppbevares som et verdidokument.
- Ved avslag sender NVE brev direkte til personen.

Sikkerhetsklareringen er gyldig i 5 år fra utstedelsesdato. Dersom det kommer nye opplysninger av betydning for personens sikkerhetsmessige skikkethet, kan klareringen suspenderes eller tilbaketrekkes.

Personer som innehar gyldig sikkerhetsklarering plikter å opplyse NVE om forhold som kan påvirke sikkerhetsklareringen. Dette kan være økonomiske, strafferettslige eller medisinske forhold, eller endring i sivilstatus. Enheten må sørge for aktiv oppfølging av dette.

6.7.3 Nærmere om autorisasjon

Før enheten gir den sikkerhetsklarerte personen tilgang til sikkerhetsgradert informasjon, skal personen autoriseres. Den som er eier av informasjonen og skal gi informasjonen til enheten, må sørge for å autorisere aktuelle mottakere. For de fleste KBO-enhetene vil dette gjelde informasjon om forsvarsanlegg, og Forsvaret skal da forestå autorisering. Se *forskrift om personellsikkerhet*, § 5. Autorisasjonen gjelder bare for tjenstlig behov. Dersom personen bytter stilling eller slutter, skal autorisasjonen tilbakekalles.

6.7.4 Nærmere om personer med utenlandsk statsborgerskap.

Utenlandske statsborgere skal ikke sikkerhetsklareres eller autoriseres etter de ovennevnte retningslinjene. En utenlandsk statsborger kan, etter *lov om forebyggende*

sikkerhetstjeneste (sikkerhetsloven) § 22 Sikkerhetsklarering av utenlandske statsborgere, gis sikkerhetsklarering etter en vurdering av hjemlandets sikkerhetsmessige betydning, samt vedkommendes tilknytning til hjemlandet og Norge. I slike tilfeller gjør OED vurderingen og gir sikkerhetsklarering. Klareringsanmodningen skal gå via beredskapsseksjonen i NVE.

§ 6-8. Sikkerhetskopier

Virksomheten skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av energiforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.

Nødvendig dokumentasjon om energisystemet og som lagres på datamedia, skal også foreligge som papirutskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted som er lett tilgjengelig for virksomheten.

6.8.1 Hensikten med bestemmelsen

Hensikten med kravet om sikkerhetskopier er å sikre at viktig informasjon for kraftforsyningens drift, gjenoppretting og sikkerhet er tilgjengelig til enhver tid ved behov. Dersom viktig informasjon (programvare, data og dokumenter) går tapt, blir feilaktig eller mangelfull, må det finnes oppdaterte sikkerhetskopier.

6.8.2 Nærmere om rutiner og kvalitet

Enheten skal ha dokumenterte systemer og rutiner for sikkerhetskopiering. Rutinene må også beskrive hvordan og hvor hyppig sikkerhetskopien skal oppdateres. Enhetens ROS-analyser skal være grunnlaget for å avgjøre omfang, hyppighet og oppbevaringstid og lagringssted. Enheten skal ha planer for gjenoppretting etter havari og skader på informasjonssystemene, jf § 2-5 Beredskapsplanlegging.

Sikkerhetskopiene skal inneholde programvare, dokumentasjon om programvare, konfigurasjonsdata og informasjon fra viktige IT-systemer for drift, sikkerhet og gjenoppretting av kraftforsyningen. Nødvendig programvare og utstyr bør være tilgjengelig, slik at gjenoppretting av viktig informasjon er praktisk mulig, også etter et totalhavari. Lagringsformatet bør være slik at informasjonen lar seg gjenopprette selv om det opprinnelige utstyret det er lagret på (både maskinvare og programvare), blir skadet eller utilgjengelig.

6.8.3 Nærmere om oppbevaring og papirkopier

Enheten må oppbevare alle sikkerhetskopier på en måte som forebygger og forhindrer tap og skade, samt sikrer tilgjengelighet. Kun autorisert personell skal ha tilgang til sikkerhetskopiene. Sikkerhetskopiene skal være sikret mot tyveri og skade, og bør lagres i et brannsikkert og avlåst sikkerhetsskap. Enheten må fjernlagre sikkerhetskopier, slik at ikke samme hendelse medfører at både original og sikkerhetskopier blir helt eller delvis utilgjengelige. Med fjernlagring menes at sikkerhetskopiene lagres i et bygg/anlegg som er fysisk atskilt fra bygget originalene oppbevares i. Sikkerhetskopier av programvare og elektronisk lagrede data bør testes regelmessig for å sikre at man kan gjenopprette og tilbakelegge programvare/data.

Hensikten med kravet om å oppbevare utskrifter er å sikre tilgjengelighet og kontinuitet dersom elektronisk lagrede utgaver er utilgjengelige (svart nett og skadete IT-systemer). Det skal til enhver tid foreligge papirkopier av de mest vitale opplysningene om kraftforsyningsanlegg og kraftsystem. Disse kan benyttes dersom IT-systemene blir utilgjengelige over lengre tid. Med vitale opplysninger menes informasjon som er nødvendig for å kunne drifte og gjenopprette kraftforsyningen. Enheten må lagre papirkopiene på et sikkert sted, samt oppdatere dem årlig og ved større endringer.

Kapittel 7. Beskyttelse av driftskontrollsystem

Pålitelige driftskontrollsystemer er avgjørende for effektiv drift, håndtering av ekstraordinære situasjoner og rask gjenoppretting av funksjon ved utfall.

Driftskontrollsystemet må virke ved langvarige og ekstraordinære hendelser.

Den raske utviklingen av teknologi og økt krav til effektivitet har ført til at man i stadig større grad kobler sammen driftskontrollsystemet med andre IKT-systemer og nettverk. Dette krever at virksomhetene må ha kontinuerlig fokus på å sikre driftskontrollsystemet mot alle typer hendelser, også uautorisert inntrengning.

Kravene i forskriften til beskyttelse av driftskontrollen er i denne forskriften mer tydelig enn i beredskapsforskriften (BfK fra 2002).

§ 7-1. Generell plikt til å beskytte driftskontrollsystemet

Alle virksomheter med driftskontrollsystem skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemer mot alle typer uønskede hendelser, herunder mot alle typer uautorisert tilgang for å hindre misbruk og spredning av ondsinnet programvare og liknende.

Alle virksomheter med driftskontrollsystem er underlagt bestemmelsene om klassifisering og sikringsplikt etter kapittel 5.

7.1.1 Hensikten med bestemmelsen

Bestemmelsen innebærer at alle virksomheter i energiforsyningen som har etablert et driftskontrollsystem, har en eksplisitt plikt til å beskytte systemet og dokumentere hvordan det er gjort. Dokumentasjonskravene framgår av § 2-10 Internkontrollsystem. Beskyttelsen skal omfatte elektroniske, administrative, organisatoriske og tekniske tiltak for å hindre urettmessig tilgang til driftskontrollsystemet.

Driftskontrollsystemet bør derfor innrettes slik at man med enkle grep kan isolere systemet fullstendig fra andre nettverk og systemer, og kunne overvåke og styre anleggene uavhengig av andre nettverk og systemer.

7.1.2 Krav for å oppfylle bestemmelsen

For mange av bestemmelsene angir forskriften konkrete, spesifikke og etterprøvbare krav til hvordan de skal oppfylles. I de tilfeller der det ikke er angitt slike krav, anser NVE at bestemmelsene er selvforklarende.

7.1.3 Definisjoner

7.1.3.1 Driftskontrollsystemet

Virksomheten er selv ansvarlig å beskrive sitt eget driftskontrollsystem, men som hovedregel er følgende en del av driftskontrollsystemet:

- Driftssentraler, datarom tilknyttet driftskontrollsystemet.

- Sambandsanlegg for overføring av styresignaler og målinger i driftskontrollsystemet.
- Programvare som benyttes til overvåking og styring av anlegg, inkludert lokale kontrollanlegg.
- Annen programvare som gjennom sin funksjon eller tjeneste er avgjørende for driftskontrollsystemets funksjon.
- Infrastruktur inkludert servere og sambandsanlegg med tilhørende komponenter.
- System, infrastruktur og sambandsanlegg som kan styre eller programmere vern med tilhørende komponenter enten gjennom driftskontrollsystemet eller gjennom andre kommunikasjonskanaler (direkte tilknytning via for eksempel Internett).
- Alle nødvendige støttefunksjoner som IKT-utstyr, nødstrøm, ventilasjon og kjøling av datarom.

Etablerer virksomheten nye koblinger mellom driftskontrollsystemet og andre typer system, eller innfører nye system som kan innvirkning på driftskontrollsystemets funksjon, er det viktig å gjøre en vurdering hvorvidt dette også skal inkluderes som en del av driftskontrollsystemet.

7.1.3.2 Driftskontrollfunksjon

I beredskapsforskriften er begrepet *driftskontrollfunksjon* benyttet flere steder. Dette forstås som følgende:

Alle organisatoriske, administrative og tekniske tiltak for å overvåke og styre anlegg i energiforsyningen.

7.1.3.3 Kontrollordninger

I flere av bestemmelsene i kapittel 7 benyttes begrepet «kontrollordninger». Kontrollordninger omfatter elektroniske, administrative og tekniske rutiner og tiltak som iverksettes for å oppfylle de enkelte krav i bestemmelsene der dette begrepet benyttes.

Eksempler på administrative rutiner og tiltak:

- Sikkerhetsregler og overordnede retningslinjer.
- Passordrutiner.
- Prosess for autorisasjon av brukere.
- Prosess for konfigurasjonskontroll av utstyr og programvare.
- Sikkerhetsavtaler med leverandører .

Eksempler på tekniske rutiner og tiltak:

- Adgangskontrollsystem.
- Teknisk autentisering av brukere og utstyr.
- Brannmurer i nettverk og konfigurering av disse.
- Logging.
- Fysisk sikring av utstyr.
- Viruskontroll og kontroll med annen skadelig programvare.
- Kontroll med nettverkstrafikk.

7.1.4 Risiko- og sårbarhetsanalyse av driftskontrollsystem

Alle som har klassifiserte driftskontrollsystemer plikter å utarbeide risiko- og sårbarhetsanalyser av sitt system i henhold til § 2-4 Risiko- og sårbarhetsanalyse. Driftskontrollsystem inngår naturlig i ”funksjoner” etter § 2-4.

For å kunne beskytte driftskontrollsystemet effektivt, må man forstå sårbarhetene i systemet dersom det utsettes for uønskede hendelser, og da spesielt store eller omfattende hendelser som kan sette systemet ut av spill i lengre tid.

Det kan være hensiktsmessig å ha større fokus på å analysere sårbarhetene og *konsekvensene* av disse enn på *sannsynligheten* for at en konkret hendelse kan inntreffe. Årsaken er at i et komplekst IKT-system med mange komponenter, med flere delsystem, og som kanskje er i kontinuerlig utvikling, vil det være tilnærmet umulig å beregne hvor sannsynlig det er at en stor, omfattende hendelse kan oppstå. Dette er diskutert nærmere under punktet om *sannsynlighet og konsekvens*.

7.1.4.1 Sårbarhet

Med sårbarhet menes driftskontrollsystemets evne til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen.

Sårbarheter kan være knyttet til for eksempel svakheter i arkitektur, programvare, infrastruktur, komponenter eller administrering og bruk av disse. Svakheterne kan medføre utilsiktede feil eller mulighet for uautorisert inntrenging.

Sårbarheter vurderes gjerne opp mot manglende barrierer som kan hindre en uønsket hendelse eller redusere mulige konsekvenser av en uønsket hendelse. Barrierene kan være av ulik art: Fysiske, programvaremessige, sikkerhetsmessige, prosedyremessige, redundans, alarmer osv.

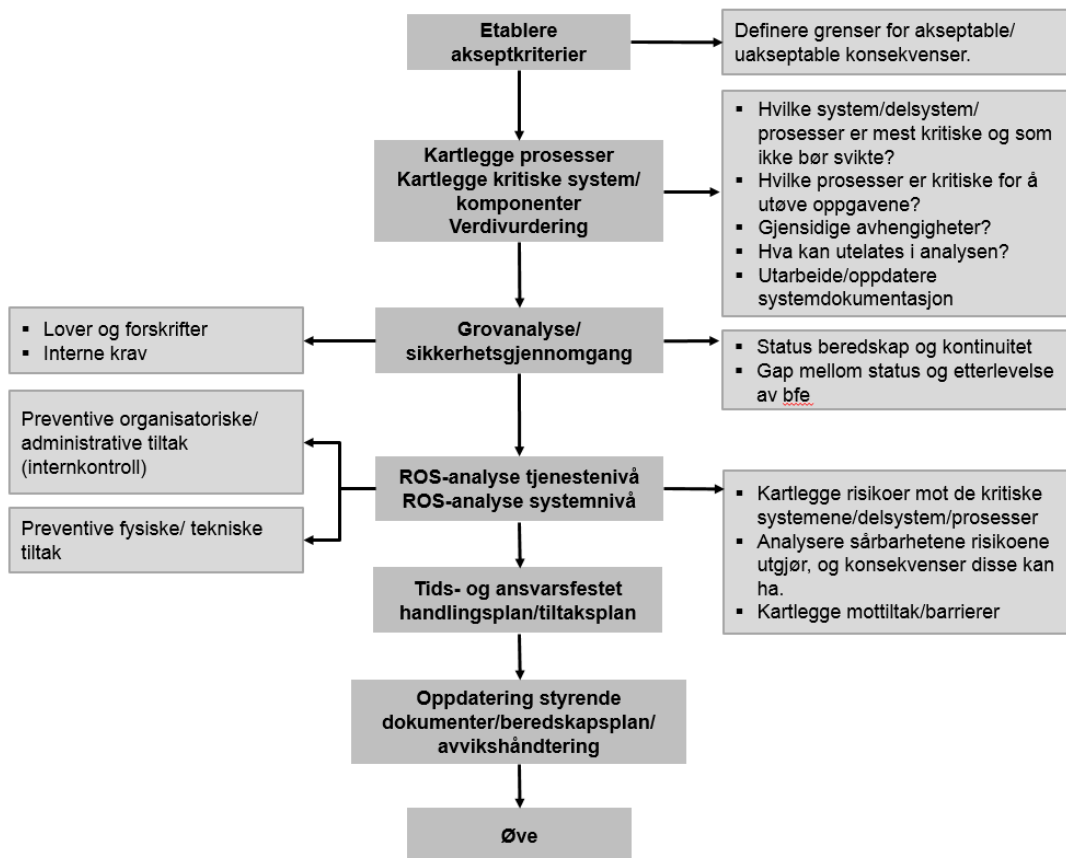
7.1.4.2 Bruk av NVEs veiledning i ROS-analyser

NVEs veiledning i risiko- og sårbarhetsanalyser fra 2010 er et rammeverk spesielt tilpasset energiforsyningen. Veiledningen har hovedfokus på analyse av fysiske objekter, men kan med tilpasninger også benyttes til å analysere driftskontrollsystemet. De viktigste tilpasningene man bør gjøre er å;

- Tilpasse metodikken til driftskontrollsystem/ IKT-system.
- Definere akseptkriteriene for risiko/ sårbarhet på en slik måte at det passer for virksomhetens IKT-systemer/ driftskontrollsystem.
- Tilpasse nivåinndelingen for ROS-analyser til driftskontrollsystem.
- Tilpasse sjekklister til virksomhetens driftskontrollsystem.

7.1.4.3 Metode

Det finnes mange metoder for risikoanalyse av IKT-systemer. I NVEs veiledning er det beskrevet en generell metode som er svært utbredt. Med utgangspunkt i den, kan en tilpasning til analyse av et driftskontrollsystem/ IKT-system se slik ut:



Figur 7-1 Eksempel på metode for risikoanalyse driftskontrollsystem/IKT-system.

7.1.4.4 Nivåinndeling - kartlegging av kritiske system/prosesser og gjensidig avhengighet

IKT-systemer er gjerne bygget opp rundt ulike komponenter, både fysiske og logiske, og noen er mer kritiske enn andre. Ofte samhandler disse komponentene seg i mellom og også ofte med andre typer systemer eller komponenter.

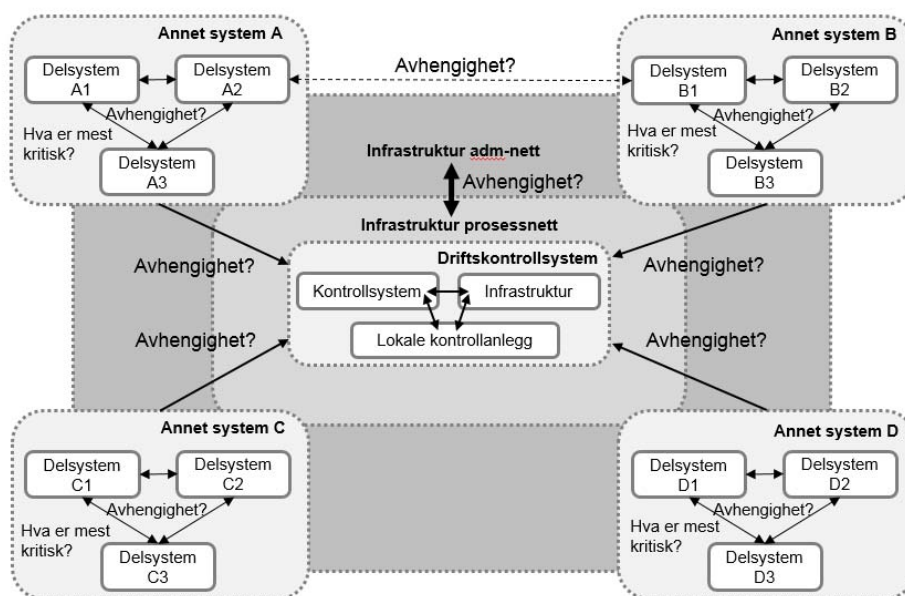
Selv om bestemmelsene i dette kapittelet i all hovedsak er rettet bare mot driftskontrollsystemet, bør man i analyseprosessen se på hele virksomhetens IKT-infrastruktur for å finne potensielle sårbarheter og mulige inngangsporter for uautorisert tilgang til driftskontrollsystemet. Årsaken til det er at det ofte foregår samhandling mellom driftskontrollsystemet og andre system eller nettverk i virksomheten. Disse koblingene bør vies stor oppmerksomhet.

NVEs veiledning for ROS-analyser viser til en nivåinndeling som kan benyttes i analyseprosessen. En tilsvarende tilnærming kan også med fordel benyttes i en analyse av driftskontrollsystemet. Dette kan gjøres i form av to nivåer, en *grovanalyse* og en *detaljert analyse*.

Grovanalysen innebærer en *kritikalitetskartlegging* av kritiske systemer og prosesser og sammenhengen mellom disse. Hensikten er å identifisere de mest kritiske systemene og hovedkomponentene i disse.

I denne fasen bør det i tillegg gjøres en vurdering av *gjensidige avhengigheter*. Man bør stille spørsmålet om det er andre systemer, som ikke er en del av driftskontrollsystemet, som ved feil eller andre hendelser kan påvirke funksjonaliteten i driftskontrollsystemet.

Nedenfor vises en prinsipiell skisse over gjensidig avhengighet mellom ulike systemer/delsystemer og driftskontrollsystemet.



Figur 7-2 Skisse som viser eksempel på gjensidige avhengigheter mellom IKT-systemer. MERK: I skissen er det brukt «system» som eksempel, men det kan også være en prosess for å utføre en handling.

Systemene som kartlegges, bør rangeres i forhold til kritikalitet. Samtidig kan man gjøre en grov risikoanalyse hvor man identifiserer de overordnede risikoer eller uønskede hendelser knyttet til systemene/hovedkomponentene.

I den **detaljerte analysen** fortas en *systemanalyse* der man går grundigere inn i hvert av de kritiske systemene for å kartlegge hvilke risikoer som kan oppstå. I dette arbeidet analyseres konsekvensene av uønskede hendelser knyttet til hver enkelt risiko og sårbarhet. Årsaksforhold og -sammenhenger må også diskuteres. I denne fasen bør man også identifisere mulige tiltak som kan redusere risikoene og sårbarhetene (barrierer).

Har man funnet gjensidige avhengigheter under kritikalitetskartleggingen, bør disse beskrives og analyseres, og det bør foreslås tiltak for å redusere sårbarhetene.

7.1.4.5 Sannsynlighet og konsekvens

Det er vanskelig å fastslå sannsynligheten for at en uønsket hendelse skal inntreffe. Enkelte feil skjer oftere enn andre, og noen ganger kan man miste kontakten med enkeltanlegg i kortere eller lengre tidsrom på grunn av feil. I tillegg kan feil med samme konsekvens være av ulik art.

Det er særdeles vanskelig å vurdere sannsynligheten for at en hendelse (eller sammenfall av hendelser) kan sette hele driftskontrollsystemet ut av spill. En av årsaken til det kan for

eksempel være at hendelsen avdekker sårbarheter som ikke er kjent fra før, eller at man faktisk ikke har opplevd såpass store hendelser tidligere.

I denne sammenhengen kan det virke mot sin hensikt å lage sannsynlighetsklasser med tidsintervaller. Én mulighet være å lage en skala uten tidfesting som et vurderingsgrunnlag for at en konkret hendelse kan oppstå.

Nedenfor er tabeller som viser eksempler på henholdsvis sannsynlighetsvurderinger, konsekvensklasser og vurdering av kritikalitet basert på en sammenstilling av sannsynlighet/konsekvens.

MERK: Eksempelene er kun eksempler, og bør tilpasses hver enkelt virksomhet basert på størrelsen/omfanget og klassen på driftskontrollsystemet. Virksomheten må selv vurdere innholdet eller hvor mange konsekvensklasser man bør bruke for sitt system.

Sannsynlighet/mulighet	Eksempel på utdypende beskrivelse
Svært lite sannsynlig	Man har ikke opplevd denne type hendelse, og heller ikke hørt om andre som har opplevd hendelsen.
Lite sannsynlig	Man har opplevd tilsvarende hendelse for lenge siden/eller ikke opplevd, men har hørt om/lest om/blitt advart om etc. at hendelsen kan oppstå.
Sannsynlig	Man har opplevd hendelsen med jevne mellomrom, men ikke ofte.
Svært sannsynlig	Dette har skjedd ofte, eller skjer ofte.

Figur 7-3 Eksempel på sannsynlighetsklasser og eksempel på utdypende beskrivelse av de ulike klasser.

Konsekvensklasse	Effekt
Kritisk	Umiddelbar stans av driftskontrollsystemet Det er ikke mulig å motta målesignaler, se tilstanden i nettet/anleggene eller sende styresignaler til anlegg. Anlegg må bemannes og styres lokalt.
Alvorlig	Tap av viktig funksjonalitet i driftskontrollsystemet. Enkelte kritiske funksjoner er satt ut av spill eller er svært ustabile, men det er fremdeles mulig å styre anlegg. Anlegg vurderes bemannet lokalt.
Mindre alvorlig	Tap av funksjonalitet som ikke er kritisk for driftskontrollsystemet Det er full funksjonalitet i driftskontrollsystemet, men enkelte forstyrrelser kan oppstå. Ikke nødvendig å bemanne anleggene lokalt.
Ingen konsekvenser	Ingen effekt på driftskontrollsystemets funksjonalitet. Risiko eller sårbarhet har ingen innvirkning på driftskontrollsystemets funksjonalitet.

Figur 7-4 Eksempel på konsekvensklasser med beskrivelse.

Kritikalitetsvurdering		
Konsekvens	Effekt	Vurdering av konsekvensreducerende tiltak
Kritisk	Umiddelbar stans av driftskontrollsystemet Det er ikke mulig å motta målesignaler, se tilstanden i nettet/anleggene eller sende styresignaler til anlegg. Anleggene må styres lokalt.	Tiltak må gjennomføres. Den uønskede hendelsen er uakseptabel og sårbarheten for høy. Selv om muligheten for at hendelsen kan inntreffe er lav, er konsekvensen såpass stor at risiko- eller sårbarhetsreducerende tiltak er nødvendig. Er ikke tiltak mulig å gjennomføre, må dette behandles i beredskapsplanen.
Alvorlig	Tap av viktig funksjonalitet i driftskontrollsystemet. Enkelte kritiske funksjoner er satt ut av spill eller er svært ustabile, men det er fremdeles mulig å styre anleggene. Anleggene vurderes bemannet lokalt.	Tiltak bør gjennomføres. Risiko eller sårbarhet er såpass stor at man bør vurdere risikoreducerende tiltak. Selv om sannsynligheten kan være liten, er konsekvensen såpass stor at risikoreducerende tiltak bør vurderes.
Mindre alvorlig	Tap av funksjonalitet som ikke er kritisk for driftskontrollsystemet Det er full funksjonalitet i driftskontrollsystemet, men enkelte forstyrrelser kan oppstå. Ikke nødvendig å bemanne anleggene lokalt.	Tiltak ikke nødvendig. Risikoen eller sårbarhet er minimal. Selv om sannsynligheten kan være tilstede, eller er stor, vil konsekvensen være såpass liten at risikoreducerende tiltak ikke er nødvendig.
Ingen konsekvenser	Ingen effekt på driftskontrollsystemets funksjonalitet. Risiko eller sårbarhet har ingen innvirkning på driftskontrollsystemets funksjonalitet.	Tiltak vurderes ikke.

Figur 7-5 Eksempel på sammenstilling av konsekvensklasser og vurdering av konsekvensreducerende tiltak knyttet til disse. I vurderingen er det også gjort en vurdering av kritikaliteten knyttet opp mot sannsynlighet. Dette bør gjøres individuelt for hver hendelse. MERK: Eksempelene er kun eksempler, og må tilpasses hver enkelt virksomhet basert på størrelsen, omfanget og klassen på driftskontrollsystemet. Virksomheten må selv bestemme innholdet eller hvor mange konsekvensklasser man bør bruke for sitt system.

7.1.5 Beskyttelse av lokale kontrollanlegg

Det lokale kontrollanlegget er kjernen i driftskontrollsystemets funksjon og må beskyttes etter samme, relevante bestemmelser som det øvrige driftskontrollsystemet. Unntaket er i § 7-14 g) Systemredundans der det er eksplisitt nevnt at systemredundansen gjelder fram til det lokale kontrollanlegget. Innen i selve lokalkontrollanlegget må virksomheten selv vurdere om det er nødvendig med redundans.

Selv om det ikke er nevnt eksplisitt i forskriften, inngår det lokale kontrollanlegget i det som i § 5-1 betegnes som "... anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger."

Plikten til å beskytte det lokale kontrollanlegget er hjemlet i § 5-1. Sikringsplikt og § 7-1 Generell plikt til å beskytte driftskontrollsystemet.

De lokale kontrollanleggene er ofte forskjellige når det gjelder alder, funksjonalitet og komponenter, og virksomhetene må selv gjøre nødvendige vurderinger om hvilke bestemmelser som er relevante for å beskytte kontrollanleggene.

Vanligvis vil det være utstyr og komponenter med eksterne innstillingsmuligheter som bør vies størst oppmerksomhet, samt intern redundans.

Utviklingen tilsier at komponentene i de lokale kontrollanleggene blir stadig mer ”intelligente” og i større grad benytter standard løsninger for programvare og protokoller for dataoverføring. Dessuten er det blitt langt vanligere å knytte anleggene til det øvrige nettverket eller til Internett for fjerninnstilling eller diagnostikk. Det betyr at virksomhetene må stille høyere krav til risiko- og sårbarhetsanalysene av de lokale kontrollanleggene.

7.1.6 Klassifisering av driftskontrollsystemet

Praksisen for å klassifisere driftskontrollsystemet er blitt noe endret i forhold til tidligere:

Hovedregler om klassifisering

- Uklassifiserte driftskontrollsystemer havner automatisk og **uten vedtak** i klasse 1. Forutsetningen er at KBO-enheten har satt i drift et IKT-basert prosesskontrollsystem for fjernstyring av anlegg. Det betyr at driftskontrollsystemet skal beskyttes i henhold til relevante bestemmelser i bfe.
- For KBO-enheter som drifter nett-, produksjons- eller fjernvarmeanlegg i klasse 2 og 3, skal driftskontrollsystemet (eller SRO-systemet for fjernvarmeanlegg) klassifiseres gjennom enkeltvedtak.
- Vedtak om klasse for driftskontrollsystem gitt i medhold av tidligere beredskapsforskrift står fortsatt ved lag inntil det blir endret eller opphevet i medhold av denne forskriften.

Vurderingen av om driftskontrollsystemet skal klassifiseres i klasse 2 eller 3 foretas gjennom en skjønnsmessig vurdering. I vurderingen inngår blant annet hvor mange anlegg som drives i de ulike klassene, samt en generell vurdering av forsyningsområdets samfunnsmessige betydning.

7.1.7 Krav knyttet til klasse

I prinsippet må virksomhetene som har driftskontrollsystem, oppfylle følgende krav avhengig av driftskontrollsystemets klasse;

- Driftskontrollsystem i klasse 1: § 7-1 til og med § 7-13.
- Driftskontrollsystem i klasse 2: § 7-1 til og med § 7-14.
- Driftskontrollsystem i klasse 3: § 7-1 til og med § 7-15.
- § 7-16 skal oppfylles av alle som har nettanlegg i regional- og sentralnettet og som har kommunikasjonsbaserte vernsystemer.
- § 7-17 skal oppfylles av alle som er avhengig av mobil radiokommunikasjon for drift og kommunikasjon i ekstraordinære situasjoner.

7.1.8 Fysisk beskyttelse av komponenter og utstyr driftskontrollsystemet, nødstrøm etc.

Driftssentral, driftskontrollrom og andre rom som inneholder prosessutstyr, nettverksutstyr for samband samt krav til nødstrøm omfattes av den generelle sikringsplikten etter § 5-1. De konkrete kravene skal utføres i henhold til bestemmelsene i kapittel 5 med vedlegg.

7.1.9 Samsvarsskjema for evaluering av hvordan bestemmelsene i kapittel 7 blir etterlevd

Som et vedlegg til veiledningen til kapittel 7 er det utarbeidet et skjema som virksomhetene kan benytte for å gjennomføre en egen evaluering av sitt driftskontrollsystem (vedlegg 14). Skjemaet kan brukes til å avdekke om man følger forskriftens bestemmelser, eller om det er gap mellom nåværende situasjon og kravene i bestemmelsene.

Skjemaet består av en rekke spørsmål knyttet til de enkelte bestemmelsene, med mulighet for å notere status og eventuelle tiltak for å oppnå samsvar med bestemmelsene.

§ 7-2. Overordnede sikkerhetsregler

Virksomheten skal fastsette sikkerhetskrav for bruk, utvikling, drift, systemvedlikehold, sikring med mer av driftskontrollsystem slik at overvåking og kontroll av energiforsyningen kan utføres på en sikker måte.

Sikkerhetskravene skal gjennomgås minimum årlig for å klarlegge om de er hensiktsmessige i forhold til virksomhetens behov, om de etterleves, og om kravene gir tilfredsstillende beskyttelse av driftskontrollsystemet.

7.2.1 Hensikten med bestemmelsen

Ved å utarbeide overordnede sikkerhetsregler må virksomheten definere hva som er sikker drift av driftskontrollsystemet. I tillegg vil reglene bidra til å gi retningslinjer for hvordan driftskontrollsystemet utformes, driftes og vedlikeholdes.

Gjennom årlige oppdateringer vil virksomheten holde oversikt over risikoene og sårbarhetene i systemet og vurdere tiltak.

7.2.2 Ytterligere veiledning - eksempler

De interne sikkerhetsreglene bør inngå som del av en samlet sikkerhetspolicy med beskrivelse av risiko, krav, tiltak og liknende samt kravene til sikkerhetsinstruks som framgår av § 6-4 Sikkerhetsinstruks (jf også § 6-5 Anskaffelser i energiforsyningen). Eksempler på innhold:

- Virkeområde og avgrensning for reglene.
- Ansvarsforhold og organisering.
- Vurdering av trusler (risiko- og sårbarhet).
- Inndeling i sikkerhetssoner, fysisk og virtuelt.
- Krav til kontroll med eksterne forbindelser, tilgang og kommunikasjon.
- Nettverk og konfigurasjonskontroll.
- Autorisasjon av og krav til rettmessige brukere.
- Administrasjon av ulike brukergruppers rettigheter, passord og liknende.
- Krav til - og avtaler med leverandører.
- Sikkerhetskopiering og forsvarlig sletting av sensitiv informasjon.
- Drifts- og sikkerhetsinstruks.
- Testing, overvåking og kontroll av sikkerhet.
- Beredskapsplan og krav til gjenoppretting av funksjon (må også inneholde planer for de mest ødeleggende scenarioene)
- Håndtering av hendelser, sikkerhetsbrudd og ekstraordinære situasjoner.

- Rutiner for evaluering, rapportering.
- Krav til informasjonssikkerhet.

§ 7-3. Dokumentasjon av driftskontrollsystemet

Virksomheten skal til enhver tid ha oppdatert dokumentasjon av driftskontrollsystemet.

I dokumentasjonen skal det inngå en oversikt over alle sikkerhetstiltak som er implementert. Dokumentasjonen skal også omfatte en oppdatert skjematisk fremstilling av driftskontrollsystemets logiske og fysiske nettverk som viser eventuelle tilgangspunkt mellom driftskontrollsystemet og andre nettverk.

7.3.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er at KBO-enheten til enhver tid skal ha full oversikt over oppbygningen av driftskontrollsystemet samt eventuelle tilkoblinger mot andre nettverk eller Internett. Videre er hensikten å dokumentere faktisk tilstand av driftskontrollsystemet og tilrettelegge for tilsyn, jf bestemmelsene i § 2-10 Internkontrollsystem.

7.3.2 Krav for å oppfylle bestemmelsen

- Dokumentasjonen av driftskontrollsystemet skal til enhver tid være oppdatert.
- Det skal utarbeides en skjematisk framstilling som viser alle hovedkomponentene og sambandet eller nettverket som binder driftskontrollsystemet sammen, samt eventuelle tilkoblingspunkter mot Internett eller andre nettverk som ikke inngår i prosessnettverket.
- Det skal utarbeides en oversikt over alle sikkerhetstiltak i driftskontrollsystemet.
- Alle planer og dokumentasjon skal inngå i virksomhetens internkontrollsystem.

7.3.3 Eksempler på dokumentasjon

- Tegninger og skisser over nettverk eller logikk i driftskontrollsystemet.
- All nødvendig dokumentasjon fra leverandører av de ulike komponentene i driftskontrollsystemet.
- Beskrivelse av virksomhetens egne konfigurasjoner av de ulike komponentene.

7.3.4 Eksempler på dokumentasjon av sikringstiltak

Nedenfor er det gitt noen eksempler på hvordan man kan dokumentere ulike sikringstiltak i driftskontrollsystemet:

På den skjematiske framstillingen:

- Plassering av brannmur(er).
- Eventuell plassering av DMZ.
- Plassering av sensorer for IDS/IPS, for enhetene som har krav om slike mekanismer.

I internkontrollsystemet (utenom den skjematiske framstillingen):

- Beskrivelse av prinsippene for nettverkssikkerhet.
- Konfigurasjoner av brannmurer, svitsjer, IDS/IPS (eventuelt prinsippene).
- Instruks for kobling mellom administrativt nettverk og prosessnett og/eller andre system.

- Beskrivelse av hvordan man fysisk har sikret de ulike komponentene i driftskontrollsystemet. Se veiledning til kapittel 5.

7.3.5 Krav om papirkopier

Det skal oppbevares papirkopier av nødvendig informasjon og konfigurasjoner av driftskontrollsystemet i tilfelle de blir utilgjengelig i elektronisk form. Dermed har man et hjelpemiddel for å gjenopprette driftskontrollsystemet ved omfattende feil. Se også veiledning til § 6-8.

7.3.6 Om omfang av dokumentasjonen

Dokumentasjonen skal:

- Være tilstrekkelig omfattende slik at personell som ikke har daglig befatning med driftskontrollsystemet relativt raskt kan sette seg inn i relevante deler av driftskontrollsystemet dersom det er nødvendig.
- Være tilstrekkelig omfattende slik at den er til hjelp ved feilsøking, endring eller ved etablering av nye konfigurasjoner, nye løsninger etc.
- Være tilstrekkelig omfattende til at man ikke er i tvil om egenskaper, konfigurasjoner eller innstillinger til prosessnettverket eller andre deler av driftskontrollsystemet.
- Være tilstrekkelig omfattende til at de setter virksomheten i stand til å gjenopprette driftskontrollsystemet etter omfattende feil, svikt eller uautorisert inntrengning.

§ 7-4. Kontroll med brukertilgang

Virksomheten skal ha kontrollordninger for tildeling, endring, sletting og vurdering av korrekt tilgang til driftskontrollsystemet.

Virksomheten skal til enhver tid kunne kontrollere hvilken person som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes.

Kontrollordningene skal gjennomgå minimum årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå.

7.4.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å etablere tiltak og barrierer for å hindre at personer som ikke er autorisert, får tilgang til driftskontrollsystemet, samt ha oversikt over hvem som er eller har vært pålogget driftskontrollsystemet.

7.4.2 Krav for å oppfylle bestemmelsen

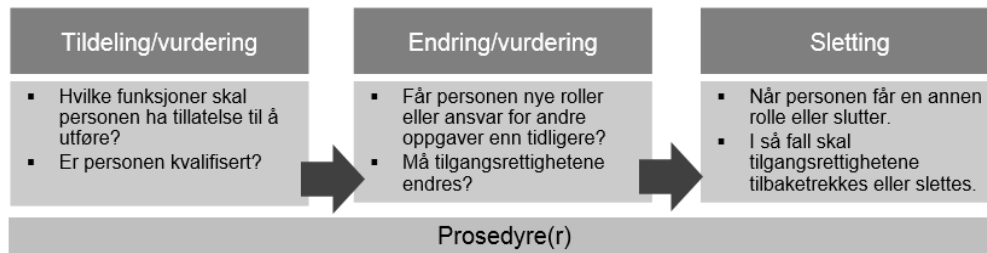
Virksomheten skal etablere følgende:

- En ordning, rutine eller prosedyre for å tildele, endre eller slette rettigheter for tilgang til de ulike delene av driftskontrollsystemet. Endringer eller sletting av rettigheter skal skje dersom personer ikke lenger har behov for rettighetene eller dersom personer slutter i virksomheten.
- En oppdatert oversikt over hvem som har tilgang til hva i driftskontrollsystemet og hvilke funksjoner de har lov til å utføre.

- En ordning for å logge hvem som har vært pålogget driftskontrollsystemet til et hvilket som helst tidspunkt.
- Det skal etableres en fast ordning der virksomheten årlig gjennomgår alle tilgangsrettigheter for å kontrollere at alle har korrekt tilgangsnivå. I gjennomgangen skal man også kontrollere at eventuelle endringer og/eller slettinger av tilgang har blitt gjennomført.

7.4.3 Eksempel på prosedyre for kontroll med brukertilgang

Nedenfor er et eksempel på elementer som bør inngå i prosedyre for tildeling, endring eller sletting av brukertilgang:



Figur 7-6 Eksempel på utgangspunktet for en prosedyre for kontroll med brukertilgang.

§ 7-5. Kontroll ved endringer i driftskontrollsystemet

Virksomheten skal ha kontrollordninger for vurdering, testing og godkjenning av endringer i driftskontrollsystemet før disse utføres, for å hindre utilsiktede feil og påføring av nye sårbarheter.

7.5.1 Hensikten med bestemmelsen

Endringer i driftskontrollsystemet kan innebære alt fra å foreta enkle konfigurasjonsendringer til å legge inn en helt ny versjon av en programvare i et system tilknyttet driftskontrollsystemet. Slike endringer kan i gitte tilfeller medføre uforutsette feil og også driftsstans. I tillegg kan endringene påføre nye sårbarheter.

Virksomheten må derfor vurdere hvilke potensielle konsekvenser endringene kan ha for funksjonalitet og eventuell sårbarhet i driftskontrollsystemet.

7.5.2 Krav for å oppfylle bestemmelsen

- Rutine eller prosedyre i internkontrollsystemet eller nedfelt i avtale med leverandør som beskriver hvordan kontroll med endringer skal foregå.
- For å hindre utilsiktede feil og nye sårbarheter, skal det utføres tester av at systemet fungerer etter hensikten også etter at endringen er utført. Endringer skal testes også etter at endringen er utført.

7.5.3 Ytterligere veiledning og eksempler

Det legges til grunn at det forut for *større* endringer er etablert prosedyrer for å gjennomføre en konkret vurdering for å kartlegge eventuelle negative konsekvenser eller skadepotensiale ved endringer. Det forutsettes også at det foreligger prosedyrer for testing slik at tiltak kan iverksettes dersom uforutsette hendelser skjer under endringsprosessen.

Med større endringer menes for eksempel:

- Oppdatering som medfører at en vesentlig del av programvaren legges inn med ny versjon (release).
- Utvidelse som medfører tilkoblinger av nye målepunkt eller sensorer for eksisterende eller nye anlegg.
- Sammenkobling for samhandling med andre nettverk, system eller prosesser.

Virksomheten bør fastsette en form for terskel for når man skal foreta en mer grundig vurdering forut for endringer.

Hva bør vurderingen omfatte?

Endringer bør vurderes ut fra hvilken innvirkning endringen får for de delene av driftskontrollsystemet som endringen omfatter, innvirkning på driftskontrollsystemet som helhet og for dem som administrerer driftskontrollsystemet. Det bør også vurderes om utstyr og nettverk er korrekt konfigurert for å kunne ta i bruk endringen.

Den kan være hensiktsmessig å benytte en form for risikovurderingsprosess når man vurderer endringen.

§ 7-6. Kontroll med utstyr i driftskontrollsystemet

Utstyr som benyttes i driftskontrollsystemet tillates ikke brukt i andre nettverk eller løsninger utenom driftskontrollsystemet, heller ikke midlertidig.

Utstyr som benyttes for å etablere logiske eller fysiske skiller mellom prosessnettverk i driftskontrollsystemet og andre nettverk, skal ha effektive kontrollordninger som hindrer uautorisert tilgang mellom skillene.

Virksomheten skal ha en oppdatert oversikt over utstyr av vesentlig betydning for driftskontrollsystemets funksjon.

Virksomheten skal ha en effektiv kontrollordning for sikker avhending av utstyr som har blitt benyttet i driftskontrollsystemet.

Det er ikke tillatt å bruke personlig eid utstyr i driftskontrollsystemet.

Bruk av trådløse datanettverk i driftskontrollsystemet er ikke tillatt.

Beredskapsmyndigheten kan i særskilte tilfeller forby bruk av utstyr.

7.6.1 Hensikten med bestemmelsen

Kontroll med utstyr og dets tilstand er svært viktig for å hindre at det for eksempel kan være en «inngangsport» for skadelig programvare, samt kompromittering av sensitiv informasjon.

Trådløse datanett forbys fordi de kan være svært sårbare for blokkering selv om de er sikret.

7.6.2 Krav for å oppfylle bestemmelsen

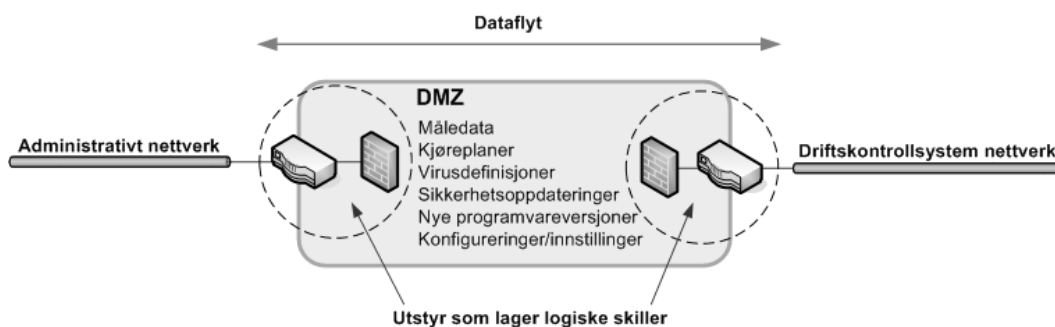
- Virksomheten skal kunne redegjøre for hvordan man sikrer at utstyr som benyttes i driftskontrollsystemet, ikke blir benyttet i andre typer nettverk.
- Der utstyr benyttes som logiske skiller mellom ulike nettverk, skal det dokumenteres hvordan man sikrer at uautorisert trafikk ikke flyter mellom skillene.
- Virksomheten skal ha en rutine eller prosedyre som sikrer at utstyr som kasseres, ikke inneholder sensitiv informasjon.
- Virksomheten skal i sitt internkontrollsystem ha en oppdatert liste over alt vesentlig utstyr i sitt driftskontrollsystem.
- Virksomheten skal i sine interne sikkerhetsregler omtale bruk av personlig utstyr i virksomheten. Det skal i reglene være et forbud mot bruk av personlig utstyr i driftskontrollsystemet.
- Det skal ikke forekomme trådløs dataoverføring (wifi eller Bluetooth) i driftskontrollsystemet – med unntak av der det benyttes for eksempel radiolinje eller satellittkommunikasjon for å overføre styringssignaler eller hente inn driftsdata i driftskontrollsystemet.

7.6.3 Ytterligere veiledning

7.6.3.1 Kontroll med utstyr

Bestemmelsens første ledd innebærer at utstyr som benyttes i driftskontrollsystemet, ikke skal benyttes i andre typer nettverk eller til andre funksjoner eller oppgaver.

Bruk av utstyr for å etablere logiske skiller mellom driftskontrollsystemet og øvrige nettverk i virksomheten, er akseptabelt såfremt virksomheten har full kontroll med at det ikke foregår uautorisert datatrafikk mellom skillene. Nedenfor er et eksempel på prinsipp der det er etablert en sone mellom det administrative nettverket og prosessnettverket for utveksling av data mellom nettverkene. Denne sonen kalles gjerne DMZ (Demilitarized Zone). I sonen blir det gjerne foretatt sikkerhetskontroll av data som skal inn i det sikre nettverket.



Figur 7-7 Eksempel på prinsipp for etablering av logiske skiller mellom prosessnettverk og administrativt nettverk. Her illustrert ved en DMZ der man foretar filoverføring mellom administrativt nett og prosessnett. I sonen kan det for eksempel også plasseres server for virussskanning, databaser etc. MERK! Dette er kun et eksempel, det finnes flere ulike typer løsninger som sikrer koblinger mellom administrativt nettverk og prosessnett. Utstyret (merket stiplet sirkel) som benyttes for å etablere logiske skiller, skal kun benyttes til dette formålet og ikke noe annet.

Hvorfor forbud mot å flytte utstyr mellom nettverkene?

Med utstyr som benyttes i et nettverk menes alt fra rutere, svitsjer og brannmurer til PCer, bærbare maskiner, nettbrett og så videre som har intern programvare som kan bli infisert av skadelig programvare eller spionvare. Risikoen er størst for det utstyret som er plassert i det administrative nettverket. Blir utstyret infisert, og flyttes til prosessnettverket, kan skadevaren eller spionvaren følge med og utgjøre en trussel mot driftskontrollsystemet.

7.6.3.2 Liste over utstyr

Bestemmelsens tredje ledd pålegger virksomheten å ha kontroll over alt teknisk utstyr i form av en liste over utstyret som inngår i driftskontrollsystemet. Hensikten er å sikre at utstyr som benyttes i driftskontrollsystemet ikke blir plassert i andre typer nettverk hvor det for eksempel kan bli eksponert mot Internett, for deretter å bli plassert tilbake i driftskontrollsystemet.

NVE presiserer at det skal utarbeides liste over alt utstyr som er av vesentlig betydning for driftskontrollsystemets funksjon. Dette innebærer også at listen skal omfatte viktig reserveutstyr.

Virksomheten må selv definere hva slags utstyr som er vesentlig. I tillegg skal det være en entydig identifikasjon av utstyret.

7.6.3.3 Sikker avhending

Sikker avhending innebærer at virksomheten må kontrollere at all informasjon om driftskontrollsystemet og annen sensitiv informasjon er betryggende slettet før utstyret avhendes. Det er viktig å merke seg at man må være spesielt oppmerksom på at SSD-disker (flashdisker) må slettes på en annen måte enn for eksempel tradisjonelle optiske disk.

7.6.3.3 Personlig utstyr

Personlig utstyr er sjelden omfattet av virksomhetenes sikkerhets- og kontrollregime og kan derfor være mer mottakelig for skadelig programvare og annet. Bestemmelsen presiserer derfor at slikt utstyr ikke tillates å bli brukt i driftskontrollsystemet.

7.6.3.4 Trådløse nettverk

Med trådløse nettverk menes for eksempel bruk av trådløse rutere for å overføre nettverkstrafikk. Slike nettverk kan sikres på en slik måte at det ikke er mulig å lese av signalene, men likevel er *signalene* svært sårbare for blokkering. Derfor anser NVE at det er nødvendig med et forbud mot bruk av slikt utstyr i driftskontrollsystemet.

Bestemmelsen gjelder ikke bruk av radiolinje eller satellittkommunikasjon for overføring av styringssignaler i driftskontrollsystemet. Virksomhetene må også være oppmerksom på at også disse signalene kan blokkeres.

7.6.3.5 Forbud mot utstyr

NVE kan forby utstyr der det kan være berettiget mistanke om for eksempel at programvaren i utstyret er manipulert av fabrikanten eller leverandøren slik at den kan benyttes i spionasje eller elektroniske angrep.

§ 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd

Virksomheten skal etablere kontrollordninger for å sikre effektiv håndtering av feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemets funksjon.

Virksomheten skal ha tilgang til tilstrekkelig personell med nødvendig kompetanse som uten unødig opphold kan håndtere forhold angitt i første ledd.

Alle sikkerhetsbrudd og hendelser skal registreres.

Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf. også § 2-6.

7.7.1 Hensikten med bestemmelsen

Å kunne håndtere IKT-hendelser er helt avgjørende for å kunne opprettholde en sikker energiforsyning. Derfor mener NVE at det er viktig at KBO-enheter med driftskontrollsystem har kontrollordninger som sikrer effektiv håndtering av feil og sårbarheter.

7.7.2 Krav for å oppfylle bestemmelsen

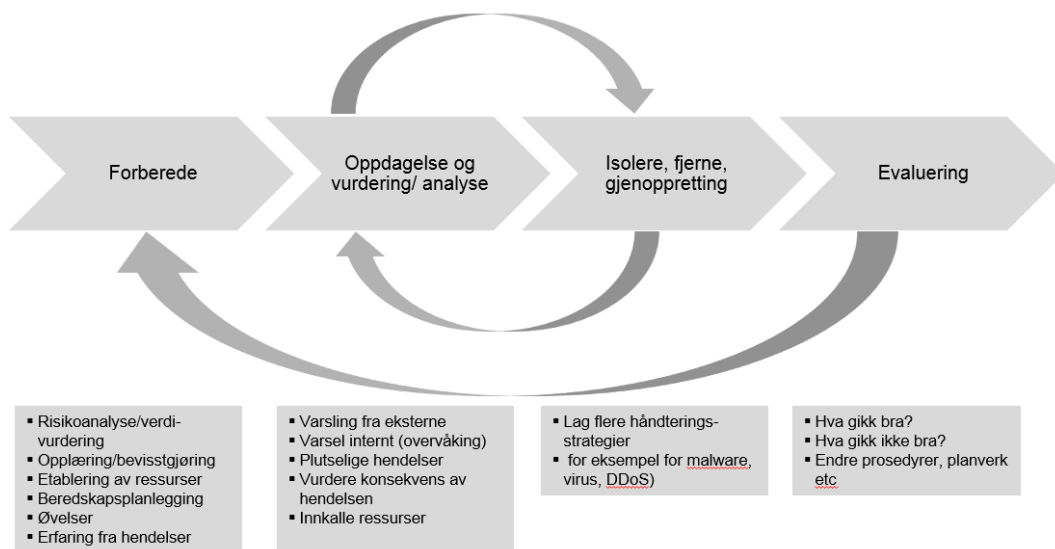
- Virksomheten skal ha rutiner eller prosedyrer for å registrere, vurdere og håndtere hendelser som kan true driftskontrollsystemets funksjonalitet. Eksempler på hendelser kan være om systemet er blitt infisert med skadelig programvare og/eller dersom uautoriserte har fått tilgang til driftskontrollsystemet – eller at en større teknisk feil oppstår.
- Med håndtering menes at virksomheten må ha etablert en prosedyre eller retningslinjer og ansvarsforhold for hvordan man skal reagere på slike hendelser. Man kan også ha en avtale med sin(e) leverandør(er) om å bli varslet dersom det oppdages sårbarheter eller liknende i utstyr eller system – og ikke minst om hvordan disse sårbarhetene skal håndteres.
- Virksomheten skal gjennom tilstrekkelig kompetanse og ressurser sikre at håndtering av feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser skjer uten unødig opphold.
- Virksomheten skal varsle beredskapsmyndigheten dersom det skjer hendelser i driftskontrollsystemet som kan utgjøre en fare for dets funksjon, og det skal foreligge en rutine for dette. Det kan for eksempel være vesentlig systemfeil som fører til tap av overvåking og kontroll over lengre tid, uautorisert inntrengning eller at annen form for skadelig programvare kommer inn i systemet.

7.7.3 Ytterligere veiledning - eksempler

7.7.3.1 Prosess for å håndtere hendelser

Det er opp til virksomheten selv å bestemme hvor stor og omfattende en slik ordning skal være, og den bør baseres på risikovurdering og hvor avhengig man er av driftskontrollsystemet. I vurderingen må man ta hensyn til hvor raskt man eventuelt kan bemanne anleggene og styre disse lokalt dersom man får svikt i driftskontrollsystemet som varer over tid.

Hendelseshåndtering kan best beskrives som en prosess der man gjennom ulike aktiviteter forbereder seg på en eventuell hendelse, oppdager, vurderer, håndterer og evaluerer hendelsen. Nedenfor viser vi et eksempel på en slik prosess:



Figur 7-8 Eksempel på prosess for å håndtere hendelser med forslag til hvordan man forbereder seg i forveien (de firkantede tekstboksene).

7.7.3.2 Ressurser

Forskriftens første ledd omfatter krav til tilstrekkelig og kompetent personell for å håndtere *feil, sårbarheter og sikkerhetsbrudd*. Ved alle disse forholdene er det viktig at man raskt får satt i gang feilsøking, feilretting slik at man kan hindre eller begrense skaden.

Det betyr at KBO-enheten enten må ha eget personell eller ha tilgang til kompetent personell gjennom avtale for å håndtere situasjonen. «Uten unødig opphold» betyr for eksempel at man i avtalen sikrer at tiden det tar før kompetent personell er på plass eller tilkoblet, blir så kort som praktisk mulig.

Det er viktig å påpeke at det som regel er ulik kompetanse som kreves for å kunne håndtere feil kontra det å håndtere sikkerhetsbrudd, selv om sikkerhetsbrudd kanskje først oppdages av driftspersonell.

§ 7-8. Beredskap og alternativ drift ved svikt i driftskontrollsystemet

Virksomheten skal ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet.

7.8.1 Hensikten med bestemmelsen

Bestemmelsen innebærer et generelt krav om at virksomheten på kort varsel skal kunne gjøre nødvendige tiltak for å drive sine anlegg selv om driftskontrollsystemet slutter å virke.

7.8.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal ha en plan for hvordan anleggene skal drives dersom driftskontrollsystemet blir utilgjengelig over lengre tid. Dette skal vurderes i risiko- og sårbarhetsanalysen.
- Man skal ha en plan for bemanning av anleggene slik at disse kan styres manuelt ved behov. Se også vedlegg 2 og 3 i beredskapsforskriften (punkt 2.1.4 i vedlegg 2 og 3.1.4 i vedlegg 3).
- I dette ligger også et krav om at det skal foreligge en plan for hvordan man i KBO-enheten kan kommunisere seg imellom og med enhetens ledelse dersom lokal bemanning er nødvendig.

7.8.3 Ytterligere veiledning

Denne bestemmelsen er i første rekke rettet mot virksomheter med driftskontrollsystemer i klasse 1. Den gir føringer for hva man må ta hensyn til dersom for eksempel driftssentralen blir utsatt for brann, eller at feil eller andre hendelser setter driftskontrollsystemet ut av spill over lengre tid. Det kan for eksempel skyldes sambandsfeil ved omfattende uvær, og man ser for seg langvarig reparasjonstid. Eller at man blir utsatt for datafeil eller dataangrep som medfører at man ikke vil benytte systemene før man er sikker på at disse er fullt ut sikre å bruke.

§ 7-9. Bemanning av driftssentral

Virksomheten skal til enhver tid ha tilstrekkelig og tilgjengelig autorisert personell med nødvendig kompetanse, slik at driftskontrollfunksjonen kan utøves uten ugrunnet opphold.

Virksomhetens risiko- og sårbarhetsanalyse skal ligge til grunn for valg av bemanningens størrelse samt omfang av ordninger for påkalling av ekstra personell ved behov, jf. § 2-4 og § 5-8.

7.9.1 Hensikten med bestemmelsen

Når det oppstår feil, er det viktig å ha operatører med god kompetanse om nettet og/eller anleggene som fjernstyres. Disse må raskt kunne vurdere feil og eventuelt koble i nettet eller operere produksjonsanlegg.

7.9.2 Krav for å oppfylle bestemmelsen

Virksomheten må:

- Ha en ordning som sørger for at operatørene i driftssentralen får tilstrekkelig kompetanse om nettet og/eller anleggene som fjernstyres, og at det foretas en form for godkjenning av dem.
- Med jevne mellomrom vurdere om operatørene har den kompetansen som er nødvendig for å utøve sin funksjon, for eksempel ved endringer i driftskontrollsystemet, innføring av ny teknologi etc.
- Virksomheten skal ha en ordning for med jevne mellomrom å vurdere i hvilken grad bemanningen er tilstrekkelig for å betjene driftssentralen, og i hvilken grad påkallingsordningens omfang er tilstrekkelig.

7.9.3 Ytterligere veiledning

Det forutsettes at virksomheten utarbeider og gjennomfører et opplegg for å lære opp og godkjenne personer som skal arbeide som operatør i driftssentralen.

Personellet på driftssentralen er de første som registrerer en hendelse, gjør de første vurderingene og innkaller øvrig personell. Dette personellet skal derfor ha:

- Kompetanse i krisemestring.
- Inngående kjennskap til virksomhetens risiko- og sårbarhetsanalyser og beredskapsplanverk.
- Være øvd i forhold til ekstraordinære hendelser.
- God oversikt over sitt forsyningsområde.
- Førstehånds kjennskap til anleggene de styrer.
- Trening i håndtering av kompliserte feilsituasjoner.
- Etablert kontakt med nødvendig personell og hensiktsmessige språkkunnskaper.
- Omfattende kunnskaper om driftskontroll.

§ 7-10. Ekstern tilkobling til driftskontrollsystem

Virksomheten skal ha kontrollordninger for å godkjenne, vedlikeholde og avvikle ordninger for ekstern tilkobling til driftskontrollsystemet, samt funksjoner for innstilling av vern. En særskilt vurdering skal ligge til grunn for godkjenning av løsning.

Kun autorisert personell kan gis adgang til driftskontrollsystemet gjennom ekstern tilgang. Virksomheten skal ha kontrollordninger for vurdering, tildeling, endring og tilbaketrekking av autorisasjon. Virksomheten skal ha en oppdatert liste over alle som er autorisert.

Det skal foreligge en egen forhåndsavtalt prosedyre for ekstern tilkobling til driftskontrollsystemet.

Det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.

For fjernvarmeanlegg der hele eller deler av driftskontrollfunksjonen utføres av selskap som ikke er KBO-enhet, må vedkommende KBO-enhet påse at hele driftskontrollsystemet beskyttes etter relevante bestemmelser i denne forskrift.

7.10.1 Hensikten med bestemmelsen

Fjerntilgang til driftskontrollsystemet kan være et svært sårbart punkt og må kontrolleres nøye. Derfor setter forskriften krav om teknisk sikkerhet og prosedyrer for oppkobling til driftskontrollsystemet via ekstern tilkobling. Bestemmelsen omfatter krav til både egne medarbeidere og eventuelt eksterne leverandører.

7.10.2 Krav for å oppfylle bestemmelsen

- Det skal utarbeides en risiko- og sårbarhetsanalyse for å kartlegge risikoer og sårbarheter knyttet til fjerntilgang. Analysen skal danne grunnlaget for tiltakene for å sikre fjerntilgangen.

- Metode og sikringstiltak som benyttes når man skal benytte fjerntilgang til driftskontrollsystemet, skal være internt godkjent av bemyndiget person eller instans.
- Det skal etableres et system eller prosedyre for vurdering, tildeling, endring og tilbaketrekking av autorisasjon av de personene som har tillatelse til å kunne koble seg til driftskontrollsystemet via fjerntilgang.
- Det skal utarbeides en egen prosedyre som skal følges, når man kobler seg til driftskontrollsystemet via fjerntilgang.
- Det skal til enhver tid være en oppdatert liste over dem som har tillatelse til å koble seg på driftskontrollsystemet.
- Fjernvarmeselskap (som er KBO-enhet) har ansvaret for å påse at alle relevante krav i forskriften følges dersom driftskontrollfunksjonen til fjernvarmeanlegget driftes av andre enn KBO-enheten, og denne ikke er KBO-enhet.

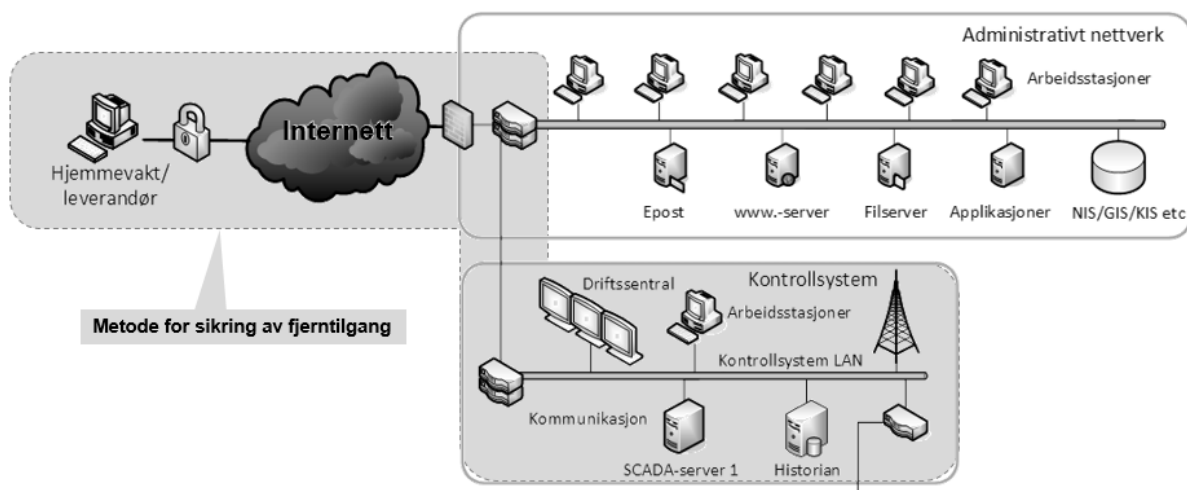
7.10.3 Ytterligere veiledning

7.10.3.1 Generelt

Generelt bør behovet for tilstandsovervåkning, og kobling samt feilretting i driftskontrollsystemet fra hjemmevakt eller leverandør vurderes strengt. Enheten må ha kontrollordninger for hjemmevakt eller leverandør som tilsvarer et beskyttelsesnivå lik det som finnes for styrings- og kontrollfunksjonene som utføres fra virksomhetens driftssentral eller øvrige lokaler.

7.10.3.2 Godkjenning av metode og sikringstiltak (av virksomheten selv)

Det som skal godkjennes, er metoden for oppkobling og tilgang til driftskontrollsystemet via fjerntilgang og hvordan denne skal sikres. Det kan illustreres slik:

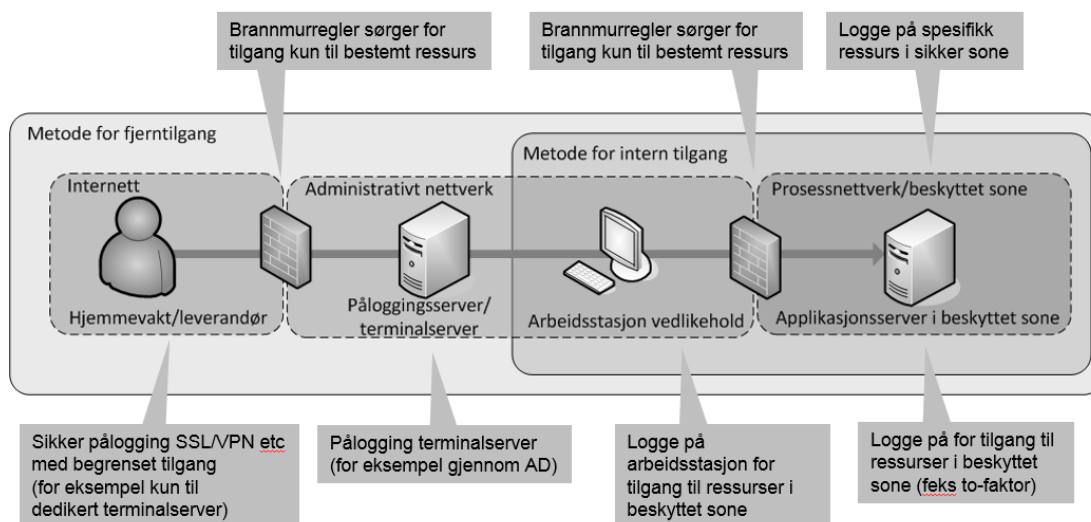


Figur 7-9 Enkel skisse som viser metode og sikringstiltak for fjerntilgang. Det grå feltet illustrerer veien å gå for å få tilgang til ressurser i kontrollsystemet.

Virksomheten må selv vurdere metoden. Det mest vanlige er å benytte en sterk bruker- og utstyrsautentisering som innebærer minimum to-nivå-autentisering av brukere ved bruk av engangspassord samt bruk av sikker kanal gjennom brannmur for kommunikasjon. Et eksempel er Virtual Private Network (VPN) med sterk kryptering av forbindelsen. For å

være sikker på at sikkerheten er fra ende-til-ende, må krypteringen også omfatte eventuelt trådløst nettverk ved fjernlokasjon.

Nedenfor viser vi et eksempel på metode for sikker pålogging:



Figur 7-10 Eksempel på prinsipp for sikker pålogging til ressurs som skal benyttes via fjerntilgang.
Kilde: NERC

7.10.3.3 Autentisering av personer som skal få tillatelse til å utføre fjerntilkobling

Autentisering av personer som skal få tillatelse til å koble seg på, kan gjøres på forskjellige måter. Uansett måte som benyttes, er hensikten med autentiseringen at de som får tillatelse til å foreta oppkobling via fjerntilgang, har fått opplæring, er innforstått med regler og prosedyrer og ikke minst er seg sitt ansvar bevisst.

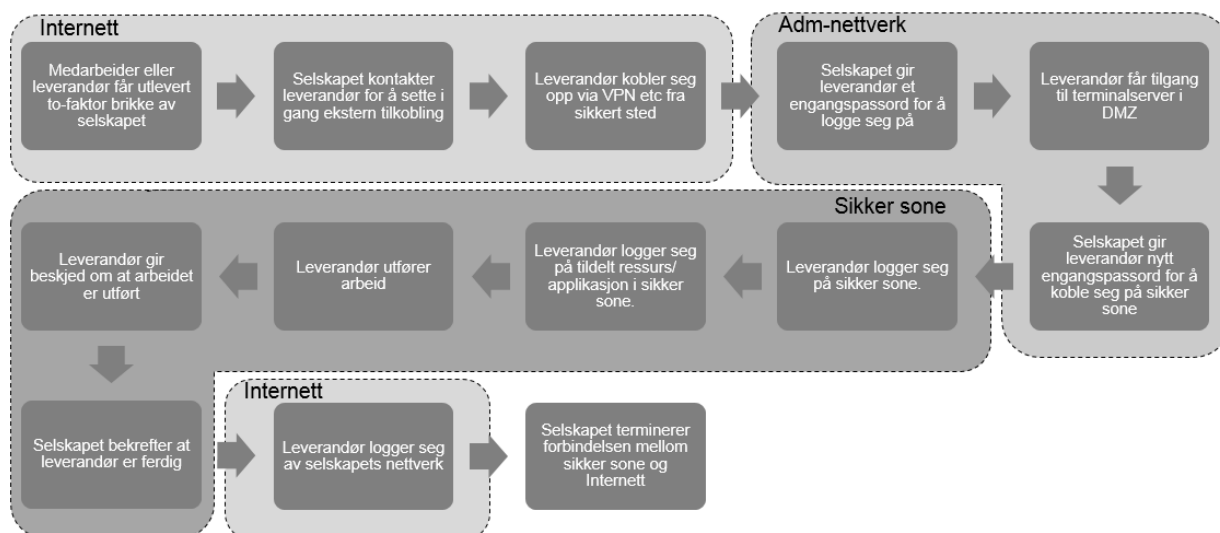
Nedenfor er noen eksempler på elementer som kan inngå i autentisering.

- Krav til å sette seg inn i prosedyrene for fjerntilgang.
- Erklæring at man har lest, forstått og vil følge reglene.
- Sikkerhetssamtale.
- Opplæring – som dokumenteres.
- Tildeling av personlige brukernavn og passord samt eventuell kodebrikke.

7.10.3.4 Prosedyre for fjerntilgang

Det skal utarbeides en tilstrekkelig detaljert prosedyre for hvordan man kobler seg opp til driftskontrollsystemet via fjerntilgang. Dette skal gjøres for å sikre at oppkoblingen skjer på samme måte hver gang slik at man ikke risikerer å omgå etablerte sikkerhetstiltak.

Virksomheten bestemmer selv hvor detaljert framgangsmåten skal være. Nedenfor viser vi et eksempel på prosedyre:



Figur 7-11 Eksempel på prosedyre for pålogging til ressurs i driftkontrollsystemet via fjerntilgang. Kilde: NERC.

7.10.3.5 Særskilt om fjernvarmeselskap

Bestemmelsens fjerde ledd setter et forbud mot at virksomheter som ikke er KBO-enheter, utøver daglig driftskontrollfunksjon. Det vil si at man ikke har lov til å sette ut denne tjenesten til ekstern leverandør. For samarbeid om driftskontrollfunksjonen mellom nettselskaper viser vi til *forskrift om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften)*.

Unntaket (femte ledd) er for fjernvarmeselskap der driften av SRO (system for styring, regulering og overvåking) utøves av for eksempel det selskapet som driver forbrenningsanlegg, og selskapet ikke er en del av fjernvarmeselskapet og heller ikke KBO-enhet.

Dette innebærer i praksis at fjernvarmeselskapet må sette krav til enheten som ikke er enhet i KBO, om å beskytte SRO-anlegget etter relevante paragrafer i denne forskriften. Dette bør avtales med det selskapet som driver SRO-anlegget.

§ 7-11. Systemredundans i driftkontrollsystemet

Virksomheten skal vurdere behovet for redundans i driftkontrollsystemet basert på lokale forhold og risikoanalyse.

7.11.1 Veiledning

Med redundans menes for eksempel redundante sambandsveier, dublering av prosessmaskiner og/eller annet vesentlig utstyr i driftkontrollsystemet.

Dersom virksomheter med driftkontrollsystem i klasse 1 vurderer at det ikke er behov for redundans, er man likevel pålagt kompensierende tiltak i form av reparasjonsberedskap. Se kapittel 4 Ressurser og reparasjonsberedskap og forskriftens vedlegg 1.

§ 7-12. Sammenkobling mellom avanserte måle- og styringssystem (AMS) og driftskontrollsystem

Dersom virksomheten har integrert funksjonalitet for bryting og begrensnings av effektuttak i avanserte måle- og styringssystem (AMS), jf. forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av netjtjenester § 4-2 e, i virksomhetens driftskontrollsystem, skal IKT-system med tilhørende utstyr som benyttes til denne funksjonen, sikres i henhold til driftskontrollsystemets klasse.

Med integrert funksjonalitet menes at funksjonen for å bryte og begrense effekt ved AMS utøves fra virksomhetens driftssentral, og at man benytter samme utstyr og infrastruktur som virksomheten benytter i driftskontrollsystemet.

Bestemmelsen gjelder til og med det utstyr eller punkt der signalene for å bryte og begrense effektuttak adskilles fra signalene i driftskontrollsystemet.

7.12.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å redusere risikoen for at uautorisert inntrengning i driftskontrollsystemet kan foregå via AMS-løsningen. I tillegg er det et mål å sikre nødvendig dialog mellom AMS- fagmiljøet og dem som har ansvar for sikkerhet i driftskontrollsystemet i forbindelse med prosjektering og innføring av AMS-løsningen.

7.12.2 Krav for å oppfylle bestemmelsen

- Dersom man kobler AMS-løsningen sammen med driftskontrollsystemet, skal man følge dokumentasjonskravene, inkludert oversikt over sikringstiltak i henhold til § 7-3.
- Det forutsettes videre at integreringen behandles i virksomhetens risiko- og sårbarhetsanalyse.
- Der AMS-løsningen og driftskontrollsystemet er integrert, skal sikringstiltakene oppfylle samme krav som driftskontrollsystemets klasse. Dette gjelder for eksempel krav til sikring av rom, skap etc.

7.12.3 Ytterligere veiledning

Målet med AMS er å få mer effektiv utnyttelse av energiresursene, et mer effektivt kraftmarked og mer gjennomsiktighet i priser, forbruk og liknende. Strømkundene skal ha kontinuerlig tilgang til all informasjon om sitt forbruk, priser og påløpte kostnader.

Imidlertid kan risikoen for feil, infisering av skadevare eller uautorisert inntrengning øke i og med at man etablerer et svært komplekst system. I tillegg kan også driftskontrollsystemet utsettes for risiko gjennom AMS-løsningen hvis AMS-løsningen kobles sammen driftskontrollsystemet.

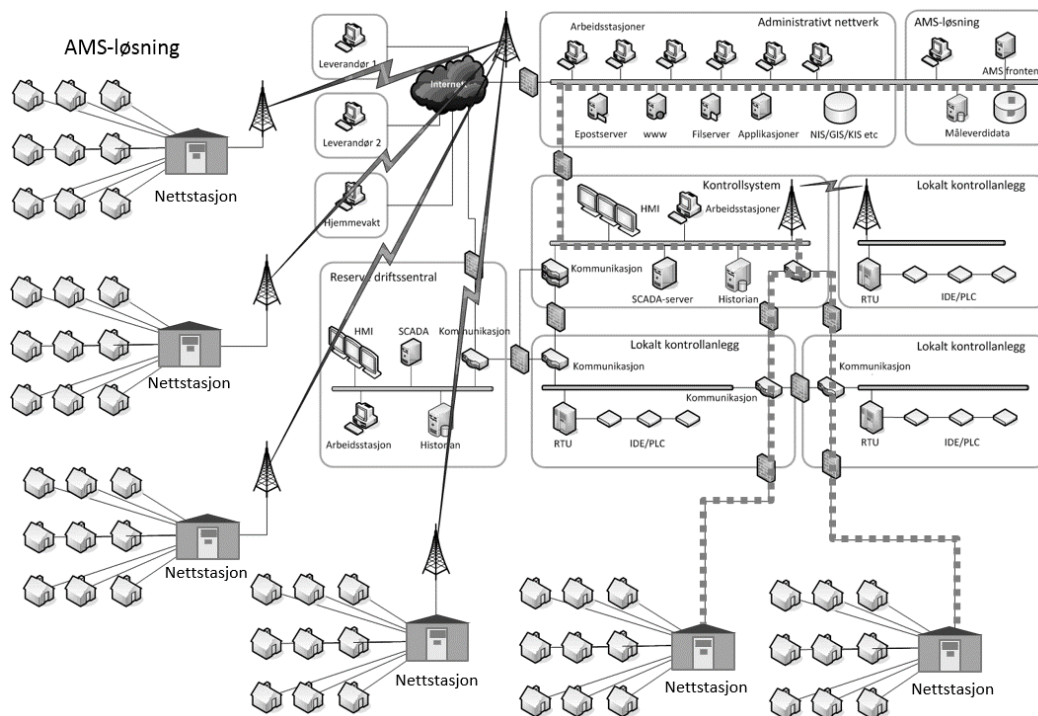
Med bryter-/ strupefunksjonalitet installert i målepunktene vil nettselskapene få mer omfattende, finmasket og oppdatert informasjon om status og driftsforhold i nettet. Med bryterfunksjon i nettstasjoner gis det mulighet for å styre nettet fra driftssentralen helt ned på kundenivå.

Dersom virksomhetene vurderer slike muligheter, må AMS-funksjonaliteten knyttet til drift- og driftskontrollsystemer risikovurderes på lik linje med driftskontrollsystemet for øvrig.

Med felles integrering av AMS-løsning og driftskontrollsystemet menes for eksempel:

- At man benytter samme nettverk og komponenter (rutere, svitsjer etc.) til toveiskommunikasjonen med AMS-løsningen og kommunikasjon med anlegg som overvåkes og styres av driftskontrollsystemet.

Prinsipielt kan dette illustreres slik:



Figur 7-12 Prinsipp for tenkt bruk av samme infrastruktur for datatrafikk til/fra AMS-løsningen og for driftskontrollsystemet. De stiplede linjene illustrerer framføring av datatrafikk fra AMS-løsningen.

Det er mulig å etablere logiske skiller i samme nettverk for overføring av AMS-signaler og signaler i driftskontrollsystemet. På den måten vil disse signalene ikke «berøre» hverandre og slikt sett være adskilt. Likevel må man være nøye med at det logiske skillet ikke brytes i for eksempel rutere, brannmurer eller svitsjer i nettverket.

§ 7-13. Beskyttelse mot elektromagnetisk puls og interferens

Virksomheten skal vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls (EMP) eller elektromagnetisk interferens (EMI). Dersom sårbarheter avdekkes, skal det gjennomføres sikrings- eller beredskapstiltak etter driftskontrollsystemets betydning for sikker drift og gjenoppretting av funksjon i energiforsyningen.

7.13.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er at alle virksomheter skal vurdere driftskontrollsystemets sårbarhet mot EMP eller EMI-hendelser. Vurderingen skal avklare om for eksempel forskriftenes generelle krav til reparasjonsberedskap er tilstrekkelig for å få gjenopprettet driftskontrollsystemets funksjon dersom utstyr blir ødelagt som følge av EMP eller EMI.

7.13.2 Ytterligere veiledning

I det moderne samfunnet, er man blitt helt avhengig av IKT for å drive samfunnskritiske funksjoner. En effektiv måte å lamme et samfunn på, kan være å benytte EMP for å ødelegge IKT-systemer og annen elektronisk infrastruktur over et stort område.

I tillegg er det blitt stadig større oppmerksomhet på hvilke konsekvenser en større solstorm vil ha på kraftnettet og ikke minst på utstyr i driftskontrollsystemene. EMP-sikring vil bidra til at gjenoppretting etter slike typer hendelser kan skje raskere.

Kravene i denne bestemmelsen er generelle og gjelder for alle virksomheter. Det innebærer at virksomhetene har en plikt til å vurdere om hele eller deler av driftskontrollsystemet er sårbart mot EMP/ EMI. Det skal gjøres gjennom risikoanalysen.

Ytterligere tiltak kan for eksempel være å oppbevare kritisk viktig utstyr eller reservedeler EMP-sikkert, som for eksempel i et EMP-skap eller i en svært godt jordnet og sikret metallkontainer.

§ 7-14. Særskilte krav til driftskontrollsystem i klasse 2

Foruten de generelle krav til beskyttelse av driftskontrollsystemet, skal virksomheter med driftskontrollsystem i klasse 2 oppfylle følgende tilleggskrav:

a. Sikkerhetskopier

Virksomheten skal jevnlig teste at gjenoppretting av elektroniske sikkerhetskopier fungerer etter hensikten.

b. Sikkerhetsrevisjon

Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene faktisk er etablert og fungerer etter sin hensikt.

c. Overvåking og logging

Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.

d. Utilgjengelig driftssentral

Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid.

e. Bemanning av driftssentral

Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold.

Virksomheten skal senest innen én time kunne bemanne driftssentralen.

Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.

f. Ekstern tilkobling til driftskontrollsystemet

Ved tilkobling fra leverandører skal driftssentralen være bemannet.

Virksomheten skal ha kontrollordning for korrekt autentisering av de personene som er autorisert til å benytte ekstern tilkobling for adgang til driftskontrollsystemet.

Virksomheten må sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheten skal utarbeide interne regler for hva som er et sikkert sted.

Den eksterne tilkoblingen skal kun åpnes når det er behov for å få tilgang til driftskontrollsystemet. Tilkoblingen skal være lukket når den ikke er i bruk.

Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling.

Dersom KBO-enheten kan foreta styring av anlegg i energiforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person.

Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

g. Systemredundans

Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett.

Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans.

Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner.

Det skal etableres reparasjonsberedskap for alt samband, jf. kapittel 4 og § 7-8.

h. Særskilt om dublering

Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil ikke rammer alle dublerte system samtidig, jf. § 7-7.

i. Beskyttelse mot EMP og EMI

Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer.

j. Sikker tidsreferanse

Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse.

7.14.1 a) Sikkerhetskopier

Virksomheten skal jevnlig teste at gjenoppretting av elektroniske sikkerhetskopier fungerer etter hensikten.

7.14.1.1 Hensikten med bestemmelsen

Testing av gjenoppretting av sikkerhetskopiene sikrer at man er trygg på at strategien for sikkerhetskopiering fungerer etter hensikten.

7.14.1.2 Krav for å oppfylle bestemmelsen

Tidfestet plan eller prosedyre for gjennomføring av testing av sikkerhetskopier.

7.14.1.3 Ytterligere veiledning

Det er ingen krav til hvor ofte man skal teste gjenoppretting av sikkerhetskopiene, men det forventes at man gjør det minimum årlig, og gjerne i form som en øvelse.

Man bør vurdere å utarbeide en strategi for sikkerhetskopier.

I strategien bør følgende inngå:

- En vurdering av hva som skal sikkerhetskopieres innenfor føringene gitt i § 6-8.
- En beskrivelse av de ulike systemer og hva slags data disse inneholder.
- En beskrivelse av teknologien som benyttes til sikkerhetskopiering.
- Prosedyrer for sikkerhetskopiering, monitorering og validering av at kopiene er korrekt utført.
- Retningslinjer for sikker lagring av sikkerhetskopiene.
- Plan for gjenoppretting av sikkerhetskopiene.

Nedenfor vises et eksempel der strategien er illustrert som en prosess:



Figur 7-13 Eksempel på strategi for sikkerhetskopiering, illustrert som en prosess.

7.14.2 b) Sikkerhetsrevisjon

Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene faktisk er etablert og fungerer etter sin hensikt.

7.14.2.1 Hensikt med bestemmelsen

Hovedmålet med revisjonen skal være å kontrollere i hvilken grad virksomheten etterlever kravene til beskyttelse av driftskontrollsystemet.

7.14.2.2 Krav for å oppfylle bestemmelsen

- Det skal utarbeides en plan for å gjennomføre jevnlig sikkerhetsrevisjon av driftskontrollsystemet.
- Det skal iverksettes korrigerende tiltak dersom det avdekkes funn under sikkerhetsrevisjonen som er brudd på forskriften.

7.14.2.3 Ytterligere veiledning og eksempler

Verktøy for styring

Den interne revisjonen er også et verktøy for å hjelpe ledelsen i virksomheten med å ha styring og kontroll over IKT-aktivitetene i tilknytning til driftskontrollsystemet.

Frekvens

Det er ingen krav til hvor ofte revisjon skal gjennomføres, men det forventes at det foretas årlige revisjoner.

Omfang

Hver revisjon trenger ikke nødvendigvis være en fullstendig gjennomgang av driftskontrollsystemet. Det kan være fornuftig å lage en revisjonsplan som strekker seg over flere år, og der man kan velge hvilke objekter som etter viktighet og funksjon skal være gjenstand for en revisjon.

Med *objekter* menes både IKT-systemer, prosedyrer, regelverk og strategier samt fysiske objekter (som for eksempel rom, skap etc.).

Revisors uavhengighet og kompetanse

Den som skal utføre gjennomgangen eller revisjonen, bør være uavhengig og objektiv i forhold til det som skal revideres. Revisor bør derfor ikke jobbe i avdelingen eller seksjonen som skal revideres, og bør heller ikke ha personlige interesser i objektene som skal revideres.

For virksomheter av noen størrelse er det ikke noe i veien for at revisor er ansatt i virksomheten selv.

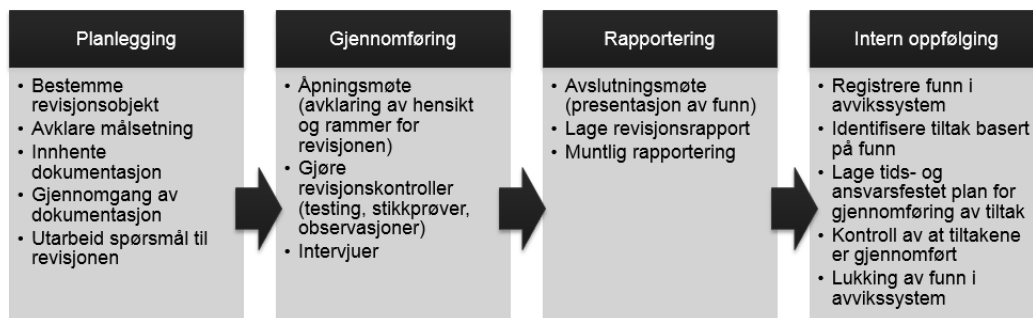
For mindre virksomheter kan det være en god løsning å benytte personer fra andre KBO-enheter til å utføre revisjonen. Dette kan bidra til at virksomhetene lærer av hverandre og finner gode løsninger på utfordringer som er like for bedriftene. Det kan også gi grunnlag for samarbeid på ulike områder.

Revisor må ha IT-kunnskaper, men trenger ikke nødvendigvis kjenne systemene som skal revideres i detalj. Revisor bør også ha kunnskap om revisjonsmetoder og teknikk for å kunne utføre revisjonen på en god måte.

Metode for sikkerhetsrevisjon

En revisjon kan utføres på mange ulike måter. Metoden må tilpasses målet for revisjonen, objektet som skal revideres og omfanget av det som skal revideres. Er målet å avdekke eventuelle brudd på retningslinjer og forskrift, vil metoden være en helt annen enn om man ønsker å finne svakheter i et system.

Likevel er det fellestrekk for alle metoder som benyttes i en sikkerhetsrevisjon. Dette kan illustreres slik:



Figur 7-14 Eksempel på rammeverk for en sikkerhetsrevisjon.

Uansett metode som benyttes, er det svært viktig at man retter oppmerksomheten mot de forholdene som er mest vesentlige eller dem som man antar utgjør størst effekt. Dette forutsetter at man vet hva som er vesentlig, noe som ikke alltid er tilfelle. Derfor vil det sannsynligvis være nødvendig å ha en bredere tilnærming for å forsøke å avdekke svakheter. Spesielt bør det legges vekt på forhold der brudd på regler eller forskrift kan få alvorlige konsekvenser.

Rapportering og håndtering av funn

For alle typer revisjoner er dokumentering av funn sentralt. Det er vanlig å utarbeide en revisjonsrapport, men det kan være vel så effektivt å legge fram funnene muntlig, etterfulgt av spørsmål og diskusjon.

Finner man forhold som helt klart er brudd på forskriften, må det gjennomføres tiltak for å lukke funnene. Tiltakene bør være tidfestet, og det bør utpekes en ansvarlig for å lukke dem. Det bør også dokumenteres.

Virksomheten kan selv vurdere hvordan eventuelle brudd på andre interne regler og retningslinjer skal håndteres.

Virksomheten må etablere et system for å registrere og følge opp funnene. Mange virksomheter har allerede et system for avvikshåndtering, og NVE anbefaler å bruke dette hvis det er mulig.

7.14.3 c) Overvåking og logging

Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.

7.14.3.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er at man ved tidlig varsling om uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet kan hindre tap av funksjon i driftskontrollsystemet eller få satt i gang feilsøking og feilretting raskest mulig.

7.14.3.2 Krav for å oppfylle bestemmelsen

- Et system som automatisk overvåker trafikk i nettverk og som gir varsler ved unormal aktivitet.

7.14.3.3 Ytterligere veiledning og eksempler

Bestemmelsen må ses i sammenheng med kravet om å etablere effektive reaksjonsrutiner for å håndtere feil, sårbarheter og sikkerhetsbrudd i driftskontrollsystemet, jf § 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd.

Mulige angrepsmetoder for å komme seg inn i et nettverk eller system har nå blitt så avanserte at normal viruskontroll i mange tilfeller ikke er tilstrekkelig til å stoppe forsøkene. For å beskytte seg mot slike hendelser, må man benytte metoder som går ut over tradisjonell beskyttelse. Automatisk overvåking av nettverkstrafikken er en slik metode.

Overvåking av nettverkstrafikk kan gjøres på forskjellige måter. De mest vanlige metodene er å benytte såkalte "Intrusion Detection System" (IDS) eller "Intrusion Prevention System" (IPS). Dette er programvare som følger med trafikken på nettverket og logger unormale hendelser. Et IDS vil kun logge hendelser, men ikke gjøre noe for å stoppe dem. Et IPS kan i tillegg sette i gang tiltak som en respons på hendelser.

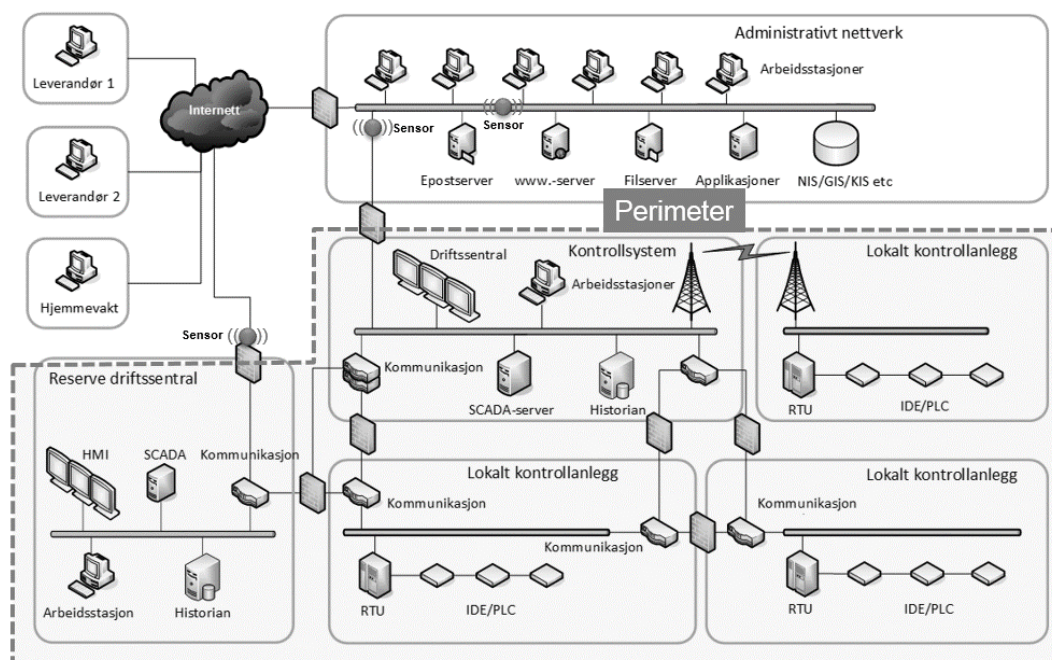
Det finnes også løsninger i moderne brannmurer og svitsjer som logger aktiviteten som foregår gjennom disse. Det kan også settes opp varsler dersom det er trafikk som ikke er godkjent.

Installering, konfigurering og innstillinger av alarmer og monitoreringsparametre i overvåkingssystem eller i brannmurer eller svitsjer kan være komplisert, og øker i kompleksitet med størrelse og omfang på driftskontrollsystemet. Blir systemene konfigurert feil, risikerer man å få mange falske alarmer, men også at systemene stopper «lovlig» trafikk i prosessnett.

Samarbeid med SCADA-leverandøren er viktig

Det er meget viktig at man samarbeider med leverandøren av SCADA-systemet når man skal etablere automatiske overvåkings- eller beskyttelsessystem i driftskontrollsystemet. På den måten kan man unngå at funksjonalitet i driftskontrollsystemet blir forstyrret eller hindret ettersom overvåkingssystemene også kan forstyrre normal prosesstrafikk.

Hvis systemet krever at man utplasserer sensorer i nettverket, må man passe på at disse ikke forstyrrer signalene for å overvåke og styre anleggene. En måte å gjøre det kan være å plassere sensorer utenfor selve driftskontrollsystemet slik at man ikke foretar analyse i dette nettverket. Dette kan illustreres slik:



Figur 7-15 Eksempel der det er etablert et "perimeter" rundt prosessnettverket som utgjør driftskontrollsystemet, og hvor sensorer er plassert rundt nett. Kulene representerer sensorer.
Kilde: NIST

I tillegg genererer overvåkingssystemene svært mange loggfiler som kan skape behov for stor lagringsplass. Derfor er det svært viktig å planlegge nøye hva man skal overvåke (hva slags trafikk) og hvor det skal overvåkes.

I tillegg vil det være nødvendig å ha kompetanse til å analysere loggene. Til dette finnes gode hjelpemidler, men det vil være absolutt nødvendig med manuell vurdering av loggene for å avgjøre om man må iverksette ytterligere undersøkelser eller umiddelbare tiltak.

7.14.4 d) Utilgjengelig driftssentral

Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid.

7.14.4.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er at virksomheten skal ha alternative måter å drive anleggene på dersom driftssentralen er ute av drift i kortere eller lengre tid.

7.14.4.2 Krav for å oppfylle bestemmelsen

I beredskapsplanen(e) eller annen dokumentasjon skal det framgå hvordan virksomheten skal overvåke og styre anleggene dersom driftssentralen blir utilgjengelig over kortere eller lengre tid.

7.14.4.3 Ytterligere veiledning

Virksomheten bør ha et alternativt sted å flytte til dersom driftssentralen blir utilgjengelig i lengre tid. Dette stedet bør klargjøres på forhånd slik at man raskt kan flytte dit. Dette innebærer at det bør plasseres utstyr, som prosessmaskiner, terminaler, skjermer etc., slik at disse raskt kan kobles opp for å gjenoppta driftskontrollfunksjonen.

7.14.5 e) Bemanning av driftssentral

Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold.

Virksomheten skal senest innen én time kunne bemanne driftssentralen.

Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.

7.14.5.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å gjøre responstiden så kort som overhodet mulig fra en hendelse varsles/oppdages til man får satt i gang tiltak.

7.14.5.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal ha en døgnskategorisk ordning der varsler om hendelser i energisystemet eller i driftskontrollsystemet mottas og umiddelbart kan vurderes av kompetent personell.
- Virksomheten skal etablere en døgnskategorisk ordning der kompetent personell skal kunne bemanne driftssentralen innen 1 time etter at varsel om hendelse i energisystemet eller i driftskontrollsystemet er mottatt.

- Virksomheten skal etablere en døgnkontinuerlig ordning for raskt å kunne trappe opp bemanning i driftssentralen eller andre sentrale funksjoner i virksomheten.

7.14.5.3 Ytterligere veiledning

Kravene i første og andre ledd innebærer at virksomheten etablerer ordninger som gjør at man kontinuerlig har personell som øyeblikkelig kan motta varsel om feil fra driftskontrollsystemet, og at disse raskt kan skaffe seg oversikt over feil og hvor de har oppstått. I tillegg stiller det konkret krav til at personen som har vakt, ikke kan være lenger unna enn at det er mulig å bemanne driftssentralen innen én time.

Siste ledd pålegger virksomheten å etablere bakvaktordninger som sikrer at ekstra personell raskt kan bemanne driftssentralen dersom det er nødvendig. Her er det ikke gitt noen tidsangivelse, men NVE forutsetter at kravene til oppmøtetid for disse ikke er lavere enn det som er angitt i første ledd.

7.14.6 f) Ekstern tilkobling til driftskontrollsystemet

Ved tilkobling fra leverandører skal driftssentralen være bemannet.

Virksomheten skal ha kontrollordning for korrekt autentisering av de personene som er autorisert til å benytte ekstern tilkobling for adgang til driftskontrollsystemet.

Virksomheten må sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheten skal utarbeide interne regler for hva som er et sikkert sted.

Den eksterne tilkoblingen skal kun åpnes når det er behov for å få tilgang til driftskontrollsystemet. Tilkoblingen skal være lukket når den ikke er i bruk.

Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling.

Dersom KBO-enheten kan foreta styring av anlegg i energiforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person.

Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

7.14.6.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er at virksomheter som gir anledning til å benytte fjerntilgang til sitt driftskontrollsystem enten for egne medarbeidere eller leverandører, gjør dette på en mest mulig sikker og kontrollert måte.

7.14.6.2 Krav for å oppfylle bestemmelsen

- Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling.
- Virksomheten skal ha ordninger, rutiner eller prosedyrer som sikrer at driftssentralen er bemannet når leverandører kobler seg opp mot driftskontrollsystemet via fjerntilgang.
- Det skal etableres ordninger eller rutiner for sikker autentisering av personene som skal koble seg til driftskontrollsystemet via fjerntilgang.
- Virksomheten skal lage regler som beskriver hva virksomheten anser som sikkert sted for å foreta oppkobling til driftskontrollsystemet via fjerntilgang.

- Virksomheten skal utarbeide prosedyrer som sørger for at den eksterne tilkoblingen er lukket, enten logisk eller fysisk, når den ikke er i bruk.
- Dersom hjemmevakten har mulighet til å foreta kobling i nettet eller styre produksjonsanlegget, skal det utarbeides retningslinjer som forteller under hvilke omstendigheter dette kan gjøres og hvordan tillatelse skal innhentes.
- Virksomheten skal ha ordninger og rutiner for å loggføre enhver påkobling til driftskontrollsystemet via fjerntilgang.

7.14.6.3 Ytterligere veiledning og eksempler

Bemanning

Første ledd pålegger virksomheten å bemanne driftssentralen når leverandører kobler seg på driftskontrollsystemet via ekstern tilkobling. Det er nødvendig for at operatøren skal kunne respondere raskt dersom en hendelse oppstår mens leverandøren er påkoblet, samtidig som operatøren kan føre kontroll med at det kun er det avtalte arbeidet som utføres.

Sikker autentisering

Andre ledd angir at virksomheten skal ha prosedyrer eller retningslinjer for å identifisere personer som skal koble seg til driftskontrollsystemet. Også denne bestemmelsen er i hovedsak rettet mot de tilfellene der leverandørene skal koble seg til.

Tilstrekkelig sikkert sted

Tredje ledd pålegger virksomheten at ekstern oppkobling skal skje fra et tilstrekkelig sikkert sted. NVE har valgt å benytte begrepet ”tilstrekkelig” da det er krevende å finne et sted der ekstern oppkobling kan skje like sikkert som fra driftssentralen.

Virksomheten skal selv lage retningslinjer for hva som godtas som sikkert sted, og formalisere dette gjennom avtaler og interne retningslinjer. Nedenfor er noen eksempler på stikkord som kan benyttes når man skal utarbeide retningslinjene:

- Krav til lokasjon.
- Krav til fysisk beskyttelse/adgangskontroll.
- Krav til beskyttelse mot innsyn.
- Krav til opplæring og/eller informasjon om rutiner eller retningslinjer.
- Krav til erklæringer fra leverandør.

NVE anbefaler en gjennomgang av relevante bestemmelser i beredskapsforskriften, og at KBO-enheten setter minimumskrav basert på disse.

Offentlige steder eller etablissementer der det oppholder seg mange mennesker anses *ikke* som sikkert sted, for eksempel:

- Flyplassterminaler
- Internettkafeer

- Bussterminaler eller togterminaler
- Restauranter, kaffebarer, kjøpesentre etc.
- Konferanser

Lukking av tilkobling

Det er viktig at den eksterne tilkoblingen ikke er åpen når den ikke er i bruk. Derfor stilles det krav om at den eksterne tilkoblingen skal åpnes kun når man kobler seg på driftskontrollsystemet via fjerntilgang. KBO-enheten må også påse at den eksterne tilkoblingen er lukket på forsvarlig måte når den ikke er i bruk. Dette gjelder både for operatørvakt, IKT-støttepersonell og leverandører.

Prosedyre

På samme måte som krav om prosedyre til § 7-10, skal også denne prosedyren være skriftlig, og den skal gjøres kjent for og benyttes av leverandører.

Tillatelse for operatørvakt til å foreta kobling

Dersom det er lagt til rette for at operatørvakten kan foreta kobling i nettet eller styre andre anlegg i energiforsyningen via fjerntilgang, skal dette kun skje etter tillatelse. Tillatelse kan være forhåndsavtalt, gjennom for eksempel retningslinjer utarbeidet på forhånd. I retningslinjene bør det stå hva som kan gjøres og under hvilke forhold. Retningslinjene skal godkjennes av en ansvarlig person.

Loggføring

Enhver tilkobling til driftskontrollsystemet skal loggføres. Hvordan loggene utarbeides, er opp til virksomheten. Som minimum forutsettes det at det framgår i loggen hvem som har vært logget på, tidspunkt for pålogging og tidspunkt for avlogging. For å få en fullstendig oversikt, og mulighet til i ettertid å undersøke hva som ble gjort, gir vi nedenfor noen eksempler på hva som bør stå i loggen:

- Tidspunkt for påkobling.
- Hvem som ga tillatelse.
- Hvem som koblet seg på.
- Årsak til påkobling.
- Tidspunkt for avkobling.

7.14.7 g) Systemredundans

Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett.

Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans.

Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner.

Det skal etableres reparasjonsberedskap for alt samband, jf. kapittel 4 og § 7-8.

7.14.7.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sikre tale- og datasamband i driftskontrollsystemet selv ved svikt i offentlige kommunikasjonstjenester eller kommunikasjonsnett eller ved andre typer feil eller hendelser. Gjennom bestemmelsen skal det samtidig sikres tilstrekkelig reparasjonsberedskap.

7.14.7.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal sørge for at sambandet er tilstrekkelig robust ved at alle sambandsknutepunkter, annet sambandsanlegg eller termineringspunkter til eller i alle anlegg i klasse 2 eller 3, utstyres med tilstrekkelig nødstrøm uavhengig av om virksomheten leier eller eier sambandskapasitet. Dersom dette ikke er mulig, skal virksomheten sørge for alternative sambandsløsninger.
- Virksomheten skal sørge for tilstrekkelig fysisk separasjon mellom de redundante sambandsveiene slik at for eksempel graveuhell eller liknende ikke setter alt samband ut av spill.
- Virksomheten må etablere reparasjonsberedskap gjennom egne eller leide ressurser slik at lokalisering av feil og reparasjon av samband kan skje så raskt som praktisk mulig.

7.14.7.3 Ytterligere veiledning

Svært mange virksomheter leier sambandskapasitet i hele eller deler av strekninger fram til anleggene som skal overvåkes og styres. For å sikre at sambandet også fungerer når leverandørens systemer svikter, må virksomheten sørge for å ha alternative løsninger for nødstrøm som umiddelbart kan ta over. Alternative løsninger kan være redundante løsninger som leies/kjøpes av ulike leverandører/tilbydere.

Redundansen skal gå helt fram til termineringspunktet som utgjør overgangen fra driftskontrollsystemet til det lokale kontrollanlegget. I det lokale kontrollanlegget kan virksomheten selv vurdere i hvilken grad anlegget skal utstyres med redundans.

En viktig grunn for bestemmelsen i andre ledd er at én hendelse ikke skal kunne sette driftskontrollsystemet ut av spill, ved for eksempel et graveuhell. Elektronisk separering som innebærer at man sender to separate signaler gjennom samme sambandsbærer, er ikke tilstrekkelig. Hvis linjen kappes, mister man begge signalene samtidig.

7.14.7.4 Krav til redundansmetoder

Å ha redundans i driftskontrollsystemet er en viktig barriere for å hindre at én enkelt hendelse setter hele funksjonaliteten ut av spill. Forskriften krever at redundansen skal oppnås ved hjelp av dubleret teknisk utstyr som prosessmaskiner, sambandsutstyr samt infrastruktur for å framføre data- og talesignaler fra sentral ledelse og ut til de enkelte anleggene i klasse 2 og 3. Sentral ledelse kan være driftssentralen eller et alternativt sted der overvåking og kontroll av anleggene foregår.

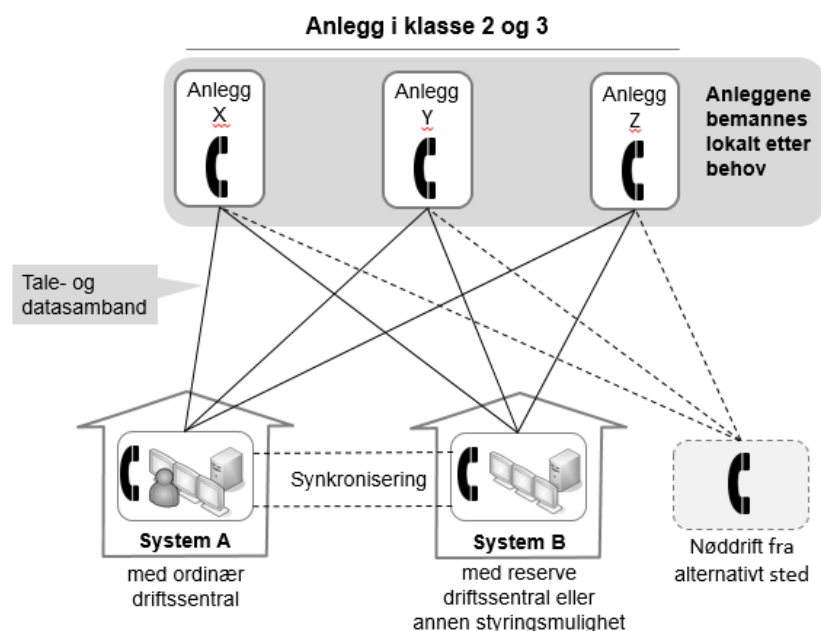
Prinsipielt kan redundans oppnås med to følgende grunnleggende metoder:

Metode 1 - Dublering på to steder

Redundansen oppnås ved at den ene prosessmaskinen med tilhørende nødvendig utstyr som sambandskomponenter, nødstrøm og kjøling, er plassert i samme bygg som driftssentralen, og den andre prosessmaskinen, med tilhørende nødvendig utstyr, er plassert i et annet bygg. Sambandet mellom begge lokasjonene er dubler, med god fysisk avstand mellom de dublerne sambandsveiene.

Delsystem A og B synkroniseres, slik at systemene kan ta over for hverandre ved feil i det ene systemet.

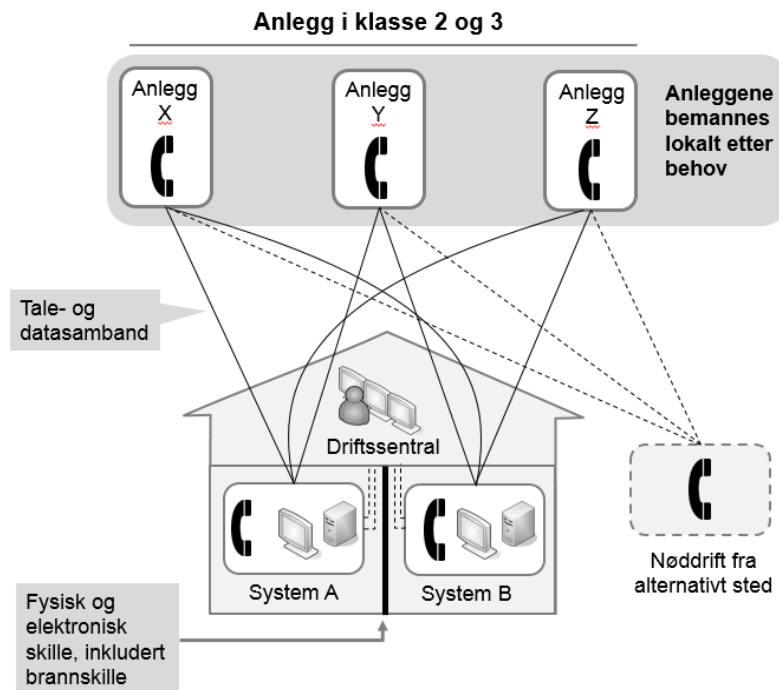
Dette er metoden som gir sikrest redundans. Er det i tillegg tilstrekkelig geografisk avstand mellom delsystem A og B, oppfylles kravet om å kunne drifte fra et alternativt sted. Det anbefales likevel at virksomheten har planer for alternativ drift dersom begge redundante systemene faller ut. Dette gjelder i særlig grad for å kunne opprettholde minimum talesamband mellom ledelsen og ut til alle anlegg i klasse 2 og 3.



Figur 7-16 Redundansmetode 1: De redundante system er plassert på hver sin lokasjon. Driftssentralen er plassert på én av lokasjonene (som eksempel), men med mulighet for styring fra den andre redundante plasseringen.

Metode 2 - Dublering og separering på samme lokasjon.

Begge prosessmaskinene er plassert i samme bygg, men med elektronisk separering slik at hver av prosessmaskinene med tilhørende komponenter er plassert i hver sin branncelle.

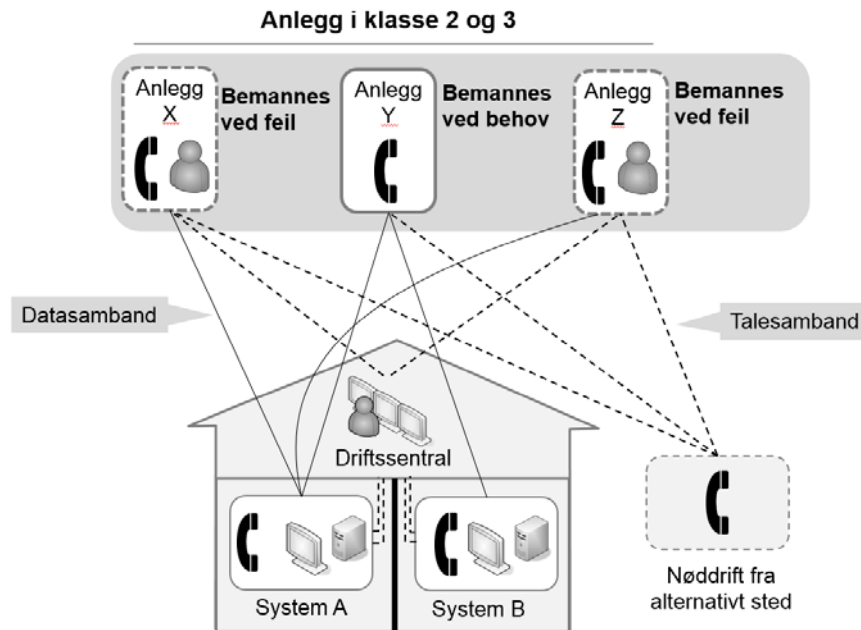


Figur 7-17 Redundansmetode 2: Begge redundante system ligger i samme bygg. De redundante system er elektronisk og fysisk adskilt, og det er et brannskille mellom de redundante systemene. Driftssentralen er i samme bygg, men med mulighet for styring ved de redundante plasseringene.

Selv om det oppnås systemmessig redundans, gir metoden dårligere sikkerhet for å opprettholde overvåking og fjernstyring dersom en hendelse setter hele bygget ut av spill og må evakueres. Virksomheter med driftskontrollsystem i klasse 2 må da i tillegg ha planer for raskt å kunne opprette nøddrift på alternativt sted. Dette inkluderer også et separat talesamband for lokalstyring fra alternativt sted til de enkelte anlegg i klasse 2 og 3, samt planer for å bemanne anlegg i klasse 2 og 3 slik at styring kan opprettholdes.

Annen metode - Driftskontrollsystem uten redundant samband til alle anlegg i klasse 2 og 3

Ved manglende redundans i driftskontrollsystemet kan det tenkes at man baserer seg på å bemanne alle anlegg i klasse 2 og 3 ved feil i systemet til de anleggene som ikke har redundant samband.



Figur 7-18 Redundansmetode der manglende redundans i driftskontrollsystemet kompenseres med planer for bemanning av stasjoner ved feil i driftskontrollsystemet.

Denne metoden oppfyller ikke forskriftens krav til å ha teknisk redundans i driftskontrollsystemet. Metoden kan kun benyttes som en nødløsning når all kommunikasjon i driftskontrollsystemet faller bort.

Dersom alt svikter – «Fallback»

Dersom hele driftskontrollsystemet faller ut, må virksomheten ha planer for en såkalt "fallback"-løsning i form av ulike alternativer og reserveløsninger eller i ulike kombinasjoner av disse metodene. Dette er mer detaljer beskrevet i veiledningen for kapittel 5.

7.14.8 h) Særskilt om dublering

Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil ikke rammer alle dublerte system samtidig, jf. § 7-7.

7.14.8.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er at virksomheten har en ordning som sikrer at systemmessige feil ved endringer i driftskontrollsystemet ikke fører til at alle redundante system faller ut.

7.14.8.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal ha prosedyrer eller andre ordninger som angir hvordan endringer skal testes og settes i produksjon på en slik måte at man hindrer hendelser som beskrevet i bestemmelsen.

7.14.8.3 Ytterligere veiledning

Dublering i driftskontrollsystemet skjer ofte ved at man har to separate, fysiske SCADA-servere eller prosessmaskiner som kan ta over for hverandre dersom den ene faller ut. De dublerede serverne er gjerne identiske, og med identisk konfigurering. Ved oppdatering oppdateres begge.

Man kan for eksempel hindre systemfeil ved endringer, ved at man oppdaterer ett system av gangen, og sørger for at dette fungerer før det andre oppdateres. Et annet alternativ kan være å teste ut endringene på et tredje system som kan fungere som et testlaboratorium.

Kravet i denne bestemmelsen må ses i sammenheng med bestemmelsen gitt i § 7-5 *Kontroll med endringer i driftskontrollsystemet.*

7.14.9 i) Beskyttelse mot EMP og EMI

Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer.

7.14.9.1 Hensikten med bestemmelsen

Utviklingen innen teknologi som kan benyttes som EMP-våpen samt sårbarheten ved bruk av radiobasert kommunikasjon i driftskontrollsystemet tilsier at det er behov for tiltak mot EMP og EMI.

Hensikten med bestemmelsen er å gi føringer for hvordan virksomheten skal innrette seg for å beskytte driftskontrollsystemet mot EMP og EMI.

7.14.9.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal sikre driftskontrollsystemet og minst 1 sambandsvei mot EMP og EMI – enten ved hjelp av konkrete EMP/ EMI-tiltak eller beredskapstiltak.
- Dersom beredskapstiltak velges, skal virksomheten kunne erstatte alt ødelagt sambandsutstyr i den sambandsveien som skal beskyttes mot EMP/ EMI.

7.14.9.3 Ytterligere veiledning

Bestemmelsen gir anledning til at beredskapstiltak, som for eksempel sikker lagring av reservedeler, kan erstatte sikringstiltak. Forutsetningen er at man lagrer tilstrekkelig med reservedeler slik at man har mulighet til å erstatte alt ødelagt utstyr i sambandsveien som skal beskyttes mot EMP/ EMI.

Se for øvrig merknad til § 7-13.

7.14.10 j) Sikker tidsreferanse

Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse.

7.14.10.1 Hensikten med bestemmelsen

Korrekt tidsreferanse i driftskontrollsystemet er viktig, særlig der ulike deler av systemene er geografisk fjernt fra hverandre, samt ved feilanalyse, avregning og driftsplanlegging.

7.14.10.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal kunne redegjøre for om de er avhengig av korrekte tidsreferanser.
- Virksomheter som er avhengig av sikker tidsreferanse, må etablere en løsning der de får tidsreferanse fra flere sikre kilder.

7.14.10.3 Ytterligere veiledning

Når GPS benyttes som eneste tidsreferanse, gir dette en usikkerhet fordi referansen kan forstyrres eller falle bort. Ved å hente tidsreferansen fra forskjellige satellitter, vil disse kunne gi ulik tid. Det er videre kjent at det er relativt enkelt å påvirke GPS-tidssignalet ved at en sterkere sender kan brukes til å overstyre et svakere satellittsignal. Det er derfor nødvendig å sikre en stabil og kontinuerlig tidsreferanse. Kontinuiteten kan oppnås ved å ha en egen klokke med stor nøyaktighet som ikke så lett påvirkes utenfra. Denne klokken kan igjen synkroniseres mot andre sikre tidsreferanser som GPS.

Kravet til tidsoppløsning følger av produktspesifikasjonene, og ikke direkte av forskrift. Enheten må imidlertid sikre at egen tidsreferanse gir tilstrekkelig oppløsning for det utstyret og de systemene som benyttes.

§ 7-15. Særskilte krav til driftskontrollsystem klasse 3

Foruten de generelle kravene samt særskilte krav til beskyttelse av driftskontrollsystem i klasse 2, skal virksomheter med driftskontrollsystem i klasse 3 oppfylle følgende tilleggskrav:

a. Reserve driftssentral

Virksomheten skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge.

Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner.

Reserve driftssentral skal utføres med sikringsnivå i henhold til vedtatt klasse for driftskontrollsystemet for øvrig, jf. § 5-6.

b. Bemanning av driftssentral

Driftssentralen skal være døgnbemannet.

Opptopping av bemanningen skal kunne skje innen én time etter at påkalling er gjort.

Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptopping av bemanning, jf. § 7-9, andre ledd.

c. Ekstern tilkobling til driftskontrollsystemet

Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.

d. Systemredundans

Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem.

Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf. kapittel 5.

e. Beskyttelse mot EMP og EMI

Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak.

I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.

f. Fastsettelse av særlige krav til bemanning

For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf. § 5-7.

7.15.1 a) Reserve driftssentral

Virksomheten skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge.

Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner.

Reserve driftssentral skal utføres med sikringsnivå i henhold til vedtatt klasse for driftskontrollsystemet for øvrig, jf. § 5-6.

7.15.1.1 Hensikten med bestemmelsen

Reserve driftssentral skal tjene som en nøddriftssentral ved for eksempel ødeleggelse, havari eller brann i samme bygning der den ordinære driftssentralen er plassert.

7.15.1.2 Krav for å oppfylle bestemmelsen

- Virksomheten skal ha en reserve driftssentral som er utstyrt og klargjort på et annet fysisk sted enn den ordinære driftssentralen.
- Virksomheten skal innrette reserve driftssentral på en slik måte at den kan være operativ så fort den er bemannet.
- Fysisk sikringsnivå, adgangskontroll etc. skal være på samme nivå som den ordinære driftssentralen og i henhold til driftskontrollsystemets klasse.

7.15.1.3 Ytterligere veiledning

Reserve driftssentral skal tjene som en nøddriftssentral, ved for eksempel ødeleggelse, havari, brann eller andre hendelser som fører til at den ordinære driftssentralen må evakueres. Reserve driftssentral skal gi beskyttelse mot hendelser som krever fysisk beskyttelse og sikring av viktige funksjoner.

Reserveløsningen som utgjør det redundante system (for eksempel reserve prosessmaskiner med tilhørende sambands/nettverksutstyr) i driftskontrollsystemet kan lokaliseres i beredskapsrommet.

Dersom man må flytte til reserve driftssentral, skal den være operativ så snart den er bemannet. Derfor bør man på forhånd gjøre følgende:

- Gjøre forberedelser for å overta overvåking og styring av anleggene fra den ordinære driftssentralen.
- Ha oppdaterte utstyrslistor og plan for utstyr som skal bli tilført fra andre steder.
- Sørge for sambandsveier, nødstrøm og øvrig nødvendig utstyr, og testing av disse med jevnlig mellomrom.
- På kort varsel kunne utstyre beredskapsrommet med de hjelpemidlene (oppdaterte kart, oversikter, sambandsutstyr og annet), som er nødvendige for å:
 - kunne lede den del av kraftforsyningen virksomheten er ansvarlig for.
 - ha løpende forbindelse med høyere og lavere ledd innen KBO.
 - kommunisere med øvrige relevante etater (politi, fylkesmenn og andre).

Det er viktig at virksomheten med jevne mellomrom øver på å flytte til reserve driftssentral, og overta styringen fra ordinær driftssentral. På den måten vil man være godt forberedt dersom behovet for å flytte oppstår.

7.15.2 b) Bemanning av driftssentral

Driftssentralen skal være døgnbemannet.

Opptrapping av bemanningen skal kunne skje innen én time etter at påkalling er gjort.

Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, andre ledd.

7.15.2.1 Hensikten med bestemmelsen

Anlegg som styres gjennom driftskontrollsystem i klasse 3, er gjerne også i klasse 3 eller så er antall anlegg såpass store at de er viktige for forsyningssikkerheten i regionen. Derfor er det nødvendig at driftssentralene i driftskontrollsystem i klasse 3 er døgnbemannet.

7.15.2.2 Krav for å oppfylle bestemmelsen

- NVE anser bestemmelsene som selvforklarende.
- I tillegg skal bemanningen om natten ha samme grunnkompetanse som øvrig bemanning, jf krav i § 7-9, første ledd.

7.15.2.3 Ytterligere veiledning

Når virksomhetene skal vurdere bemanningens størrelse, bør det tas utgangspunkt i evalueringer etter hendelser, ROS-analyser etc. for å vurdere hvorvidt bemanningen har vært tilstrekkelig til å kunne håndtere de hendelsene som har vært.

Følgende spørsmål kan være aktuelle å stille seg ved vurderingen:

- Kunne hendelsene vært håndtert raskere/bedre med større grunnbemanning i driftssentralen?
- Hadde operatørene god nok kompetanse og evne til å håndtere hendelsene, eller vil de kunne håndtere hendelser som kan forventes å oppstå i henhold til ROS-analysen?
- Har virksomheten planer for å utvide nettet eller driftskontrollsystemet som kan tilsi at man trenger større grunnbemanning?

Dersom virksomheten finner ut at det ikke er nødvendig med økt bemanning, anbefales det sterkt at man med jevne mellomrom øver operatørene i å håndtere feilsituasjoner.

7.15.3 c) Ekstern tilkobling til driftskontrollsystemet

Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.

7.15.3.1 Hensikt med bestemmelsen

Anlegg som styres gjennom driftskontrollsystem i klasse 3, er gjerne også i klasse 3 eller så er antall anlegg såpass store at de er viktige for forsyningssikkerheten i regionen. For å ivareta sikkerheten, og det faktum at driftssentralen i disse driftskontrollsystemene er døgnbemannet, gis det gjennom bestemmelsen et klart forbud mot å koble i anlegg gjennom fjerntilgang.

7.15.3.2 Krav for å oppfylle bestemmelsen

- NVE anser bestemmelsen som selvforklarende.

7.15.3.3 Ytterligere veiledning

For krav om veiledning for oppkobling for leverandører, se krav og veiledning til § 7-14 f).

7.15.4 d) Systemredundans

Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem.

Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf. kapittel 5.

7.15.4.1 Krav for å oppfylle bestemmelsen

- Krav til hvordan bestemmelsens første ledd skal oppfylles, anses som selvforklarende.

- Virksomheten skal i minst én sambandsvei til alle anlegg i klasse 3 ha eksklusiv rett til å bestemme over transmisjonslinjer og komponenter i sambandsveien som virksomheten leier. Videre skal virksomheten ha eksklusiv rett til å bestemme hvem som skal ha fysisk tilgang til ovennevnte. Med å bestemme menes at virksomheten skal ha rett til å bestemme hvem andre som kan leie kapasitet i eller få fysisk tilgang til sambandsveien eller komponenter.

7.15.4.2 Ytterligere veiledning

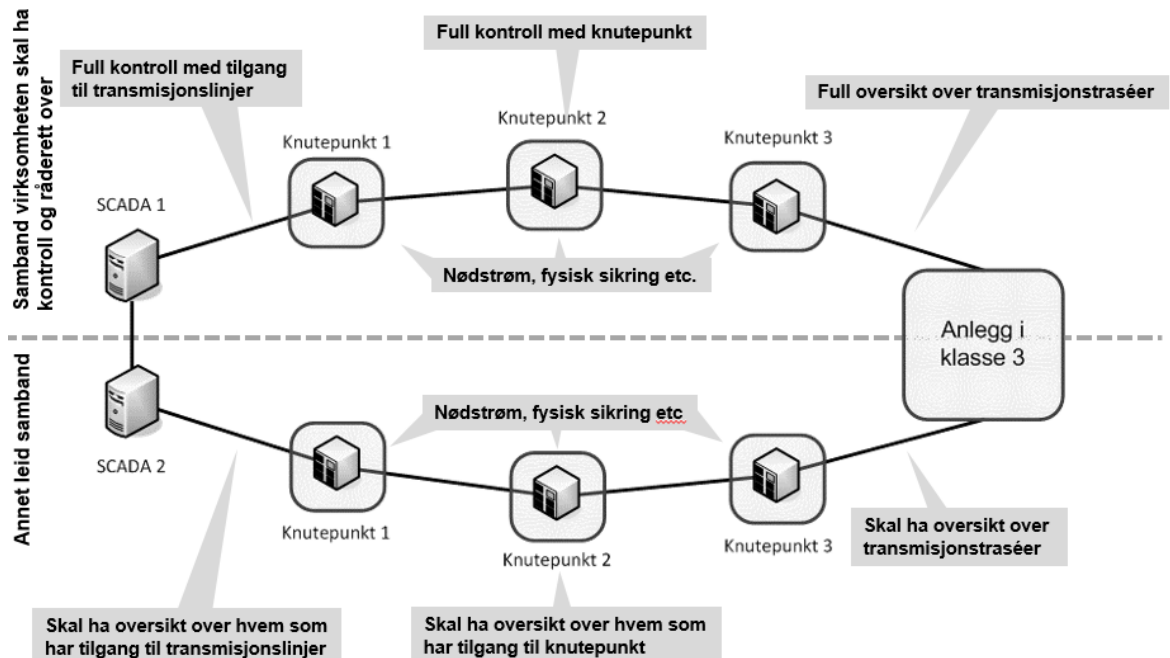
Første ledd krever at de redundante sambandsveiene har såpass lang avstand fra hverandre at samme hendelse ikke slår ut begge eller alle dersom det er etablert ytterligere redundans. Virksomhetene bør også vurdere å bruke ulike metoder for redundant samband, for eksempel radiolink, satellitt etc.

Virksomheten kan velge enten å eie eller leie de fysiske transmisjonslinjene (for eksempel fiberlinjer) i alle redundante sambandsveier. Likevel må virksomheten gjennom avtalen med leverandøren sørge for å få full råderett over den fysiske transmisjonslinjen, gjennom å leie såkalt svart fiber i minst én sambandsvei. Videre må virksomheten sørge for tilstrekkelig reparasjonsavtale ved for eksempel brudd i sambandslinjene de leier.

Det er krav om at alt teknisk utstyr som kobles på sambandslinjene i én sambandsvei, skal beskyttes etter relevante krav i forskriften. Særlig gjelder det kravene til fysisk beskyttelse og nødstrøm etter bestemmelsene i kapittel 5 med vedlegg.

Likedan må virksomhetene sørge for å ha oversikt over de fysiske føringsveiene til linjene de leier, for å sikre stabil drift og tilstrekkelig fysisk separasjon.

Eksemplet under viser prinsippet for å overholde kravet i bestemmelsen:



Figur 7-19 Prinsipp som viser forholdet mellom å ha kontroll og råderett over samband og det å ha annet leid samband.

7.15.5 e) Beskyttelse mot EMP og EMI

Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak.

I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.

7.15.5.1 Hensikten med bestemmelsen

Se hensikten med § 7-14 i).

7.15.5.2 Krav for å oppfylle bestemmelsen

- Komponenter og annet utstyr i driftskontrollsystemet som kan bli påvirket av en EMP/ EMI-hendelse, og utstyr og komponenter i minst én sambandsvei til alle anlegg i klasse 3 skal være omfattet av EMP/ EMI-beskyttelse.
- Alternative beskyttelsestiltak for sambandsvei til anlegg i klasse 3 skal være forhåndsgodkjent av NVE.
- Komponenter og annet utstyr som kan bli påvirket av en EMP/ EMI-hendelse i minst én sambandsvei til alle anlegg i klasse 2, skal være omfattet av EMP/ EMI-beskyttelse eller alternativ beskyttelse.

7.15.5.3 Ytterligere veiledning

I følge bestemmelsen plikter enhetene å EMP/ EMI-beskytte utrustning i driftskontrollsystemet for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Imidlertid åpnes det for at NVE i særskilte tilfeller etter søknad kan godkjenne beredskapstiltak som alternativ til sikringstiltak. NVE forutsetter at det blir gjennomført en risiko- og sårbarhetsanalyse knyttet til vurderingen dersom virksomheten ønsker å ha beredskapstiltak som erstatning for EMP/ EMI-sikring.

Søknaden bør inneholde:

- ROS-vurdering.
- Beskrivelse av beredskapstiltakene.
- Hvordan eventuelt reservedeler oppbevares EMP/ EMI-sikkert.
- Gjenopprettingstid ved bruk av beredskapstiltakene.
- Begrunnelse for hvorfor man velger beredskapstiltak og ikke EMP/ EMI-sikring.

Når NVE vurderer søknaden, vil vi blant annet se på hvorvidt enheten allerede har etablert redundans i form av ekstra EMP/ EMI-sikring av lokaler eller EMP/ EMI-sikker oppbevaring av reservedeler.

Forutsetningen for å kunne etablere beredskapstiltak i stedet for EMP-sikring er at man lagrer tilstrekkelig med reservedeler slik at man har mulighet til å erstatte alt ødelagt utstyr i sambandsveien som skal beskyttes mot EMP/ EMI.

Det er ikke NVEs hensikt å gi anledning til å erstatte *all* EMP/ EMI-beskyttelse med beredskapstiltak. NVEs praksis vil være å godkjenne beredskapstiltak der det er mest hensiktsmessig, for eksempel for anlegg som er lett tilgjengelige, og der det av plass- eller bygningsmessige hensyn vil være uforholdsmessig dyrt å etablere EMP-sikring. NVE forutsetter videre at man ved større ombygginger, moderniseringer eller nybygg etablerer fullverdig EMP/ EMI-sikring der det tidligere er etablert beredskapstiltak.

NVE forutsetter videre at allerede etablert EMP/ EMI-sikring, for eksempel EMP-rom, opprettholdes og vedlikeholdes i henhold til bestemmelsene i § 5-1, 1. til 3. ledd.

7.15.6 f) Fastsettelse av særlige krav til bemanning

For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf. § 5-7.

7.15.6.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å gi NVE hjemmel til å fastsette gjennom enkeltvedtak særskilte krav til beskyttelse og bemanning utover gjeldende bestemmelser. Det gjelder for KBO-enheter med driftskontrollsystemer som er særlig viktige for landets energiforsyning.

§ 7-16. Vern av kraftsystem i regional- og sentralnettet

Kommunikasjonsbaserte vernsystemer i sentral- og regionalnett skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftforsyningssystemet.

7.16.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sette krav til funksjon av viktige vernsystemer og sikkerhet i kommunikasjon i de viktigste vernsystem samt eventuell fjerninnstilling av vern.

7.16.2 Krav for å oppfylle bestemmelsen

- Første ledd: sambandet mellom kommunikasjonsbaserte vern og kommunikasjon for fjerninnstilling av vern, der det benyttes, skal beskyttes mot uautorisert tilgang for å hindre misbruk og/eller manipulering av signaler og meldinger til driftssentralen.
- Andre ledd: NVE anser denne som selvforklarende.

7.16.3 Ytterligere veiledning

Bestemmelsen omfatter kun vern i anlegg i regional- og sentralnettet.

Krav til vern er i dag gitt i *systemansvarsforskriften* § 20 Vern og reléplanlegging og i § 21 Systemvern. Dessuten stilles det krav til vern i *forskrift om elektriske forsyningsanlegg* § 2-11 Overvåking og kontrollsystemer og i § 4-10 Vern, kontroll og hjelpesystemer. I disse forskriftsbestemmelsene er det krav om å ha fungerende vernsystemer, men det er

ikke særskilte krav for de aller viktigste vernsystemene. Det er heller ingen krav til beskyttelse av kommunikasjonen vernsystemene i mellom eller for kommunikasjonen som benyttes for fjerninnstilling av vern.

Sikker kommunikasjon

Fjerntilgang til vernsystem kan være et svært sårbart punkt og må kontrolleres nøye. NVE forutsetter at kommunikasjonen beskyttes i henhold til relevante bestemmelser i forskriften. Se veiledning for § 7-10 for eksempler.

Vernfunksjon

NVE mener at gjeldende prinsipp om å benytte ett differensialmålede uforsinket vernsystem for samleskinner videreføres. Dette gjenspeiles også i *funksjonskrav i kraftsystemet* (FIKS).

Når det gjelder krav til systemvern, anser NVE at dette er tilstrekkelig dekket gjennom *forskrift om systemansvaret*, og Statnetts funksjonskrav i FIKS.

§ 7-17. Mobile radionett – driftsradio

Alle enheter i KBO som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon, skal ha tilgang til et mobilt sambandssystem. Dette sambandssystemet skal:

- a. Omfattes av den generelle sikringsplikten etter § 5-1.*
- b. Til enhver tid holdes i funksjonsdyktig stand, være klar til bruk, og det skal være rask tilgang på kritiske reservedeler og kompetanse på feilretting.*
- c. Kunne betjenes av personell med nødvendig kompetanse til bruk.*
- d. Ha tilstrekkelig dekningsgrad for kraftforsyningens anlegg og drift.*
- e. Kunne fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett.*
- f. Ha tilstrekkelig nødstrøm ved omfattende eller langvarige strømbrudd, herunder et nødstrømssystem med automatisk start og minimum 48 timer selvstendig driftstid.*
- g. Ha nødvendig funksjonalitet med blant annet direkte apparat til apparat-kommunikasjon, gruppesending og felles oppkall.*
- h. Kunne fungere som reservesamband om annet viktig samband svikter.*
- i. Der hvor radionettet benytter anlegg tilhørende et klassifisert driftskontrollsystem eller hvor det må regnes som en del av dette, skal sambandssystemet beskyttes i henhold til driftskontrollsystemets klasse.*
- j. Der hvor radionettet er digitalisert og f.eks. baserer seg på IP-løsninger, skal dette sikres mot uautorisert tilgang, spredning av uønsket programvare, urettmessig overtakelse m.m. etter relevante bestemmelser i denne forskrift.*

7.17.1 Hensikten med bestemmelsen

Hensikten med bestemmelsen er å sikre at de virksomhetene som er avhengig av mobilkommunikasjon anskaffer, driver, bruker og vedlikeholder et mobilt sambandssystem.

7.17.2 Krav for å oppfylle bestemmelsen

NVE anser at bestemmelsen angir kravene på en tilstrekkelig selvforklarende måte.

7.17.3 Ytterligere veiledning

NVE vil påpeke at bestemmelsen om mobilt radionett er teknologinøytral og setter ingen begrensninger på virksomhetene i valg av system så lenge kravene i bestemmelsen og andre relevante krav i denne forskriften oppfylles.

For å sikre uavhengighet i forhold til funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett, må virksomheten sørge for tilstrekkelig med nødstrøm og også sikre radiostasjoner/-hytter mot innbrudd, hærverk og sabotasje.

Nødstrøm

Ordinær strømforsyning, nødstrøm og samband bør føres inn i bygninger gjennom jordkabler. Stasjonens kabling bør organiseres slik at den beskytter mot overspenninger. Sikringsskap og liknende plasseres innendørs. Likerettere bør dupliseres og overvåkes med alarmer.

Stasjonene bør utstyres med batterianlegg med driftstid på minst 72 timer. Alternativt kan stasjonen ha batterianlegg med driftstid på minst 48 timer dersom stasjonært nødstrømsaggregat er installert. Krav til nødstrøm kan reduseres dersom man har god adkomst til stasjonen.

Klassifisering

Mobilt radionett blir normalt ikke klassifisert og er som sådan ikke en del av et klassifisert driftskontrollsystem, da det nødvendigvis ikke er sammenheng mellom driftskontrollsystemets betydning og radionettets betydning.

Dersom man likevel, i tillegg til talekommunikasjon, benytter radiosystemet til overføring av signaler til driftskontrollsystemet eller andre typer viktige signaler, må man i tillegg oppfylle relevante krav til beskyttelse i henhold til bestemmelsene i beredskapsforskriften. Dette gjelder særlig krav om redundans, særskilte krav til fysisk beskyttelse samt beskyttelse mot IKT-trusler (se avsnitt om digitale sambandsløsninger).

Man bør også vurdere redundans ved for eksempel å ha to overføringsmuligheter i viktige dekningsområder, uavhengig om man benytter radiosystemet til andre formål enn talesamband.

Fysiske sikringstiltak

- Viktige og utsatte stasjoner bør bygges i betong, eventuelt stålkontainer (dette gir bl.a. beskyttelse mot brann, innbrudd og hærverk).
- Viktige komponenter bør plasseres i avlåste telerom uten vinduer, med innbruddsalarm til døgnbemannet sentral (eventuelt hjemmevakt).

- Vinduer bør tildekkes med solide lemmer, låst eller boltet til innsiden.
- Kabelføringer til mast bør føres i tildekket kanal eller i kabelbro slik at de ikke er lett tilgjengelige for uvedkommende.
- Jordkabler bør beskyttes mekanisk ved at de legges i egne rør eller betongkanaler
- Antenner og master er vanskelige å beskytte. Her bør det anskaffes reserveutstyr og også tilrettelegge for alternative føringsveier for kommunikasjon.
- Master bør beskyttes med klatrehindre.
- Alle rom som inneholder elektronisk utstyr og som har betydning for driften av driftsradiostasjonen (telerom og liknende), skal gjennom ROS-analyse vurderes skjermet mot EMP/EMI, jf § 7-13 Beskyttelse mot elektromagnetisk puls og interferens.

Beskyttelse av digitale sambandsløsninger

Digitale sambandsløsninger benytter tradisjonell IKT-teknologi som for eksempel overføring via IP, standard operativsystem etc. Dette kan utsette både selve radiosystemet og sambandstrafikken for ulike trusler på linje med andre IKT-systemer, og krever at man tenker gjennom hvordan man skal beskytte systemet mot dette. Man bør derfor gjennomføre en analyse som blant annet kartlegger hvilke bestemmelser i kapittel 7 man bør følge for å beskytte radiosystemet mot å bli utsatt for IKT-trusler.

Dette bør også diskuteres inngående med leverandør/produsent.

Eksempler på hva som bør vurderes:

- Tilgangskontroll.
- Krav til kontroll ved fjerntilgang fra leverandør.
- Hindre at skadelig programvare kommer inn i systemet.
- Sikkerhet ved sammenkobling mellom system for radiokommunikasjon og andre system/nett.
- Kontroll med endringer i programvare etc.

Reservedeler og reparasjonsberedskap

Virksomheten bør inkludere reparasjon av driftsradioanlegg i sin beredskapsplan, og ha et relevant lager av de mest utsatte komponentene i radiosystemet. Der det benyttes viktige enheter med svært lang leveringstid, bør leverandøren kontaktes for å inngå avtale om lagerhold. Egne medarbeidere bør ha tilstrekkelig kompetanse for enkel feilsøking og -retting. Ved behov for assistanse, avtales dette med leverandør eller andre med som har tilstrekkelige kvalifikasjoner.

For krav til nødvendig kompetanse for å installere utstyr i radioanlegg vises det til *lov om elektrisk kommunikasjon (ekomloven)* § 2-14, med tilhørende forskrifter; *forskrift om elektroniske kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften)* kapittel 9, samt *forskrift om autorisasjon for installatør av elektronisk kommunikasjonsnett og radioutstyr (autorisasjonsforskriften)* kapittel 9.

Kapittel 8. Avsluttende bestemmelser

Kapitlet beskriver hvilke sanksjonsmuligheter som kan benyttes ved overtredelse av de ulike bestemmelsene i forskriften. Kapitlet inneholder i motsetning til BfK fra 2002 ikke en egen bestemmelse om klageadgang. Klageadgangen følger fortsatt av § 6 i *lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)*.

Det er bare avgjørelser som er enkeltvedtak etter *forvaltningsloven*, som kan påklages. Enkeltvedtak som er fattet med hjemmel i beredskapsforskriften kan, etter *forvaltningsloven* § 29, påklages til OED innen tre uker fra det tidspunktet underretningen om vedtaket er kommet fram til vedkommende part. Nærmere vilkår for klagerett er regulert i *forvaltningsloven* § 6. En eventuell klage innebærer ikke uten videre at gjennomføringen av vedtaket utsettes. NVE kan beslutte å gi en klage utsettende virkning etter *forvaltningsloven* § 42. Enheten kan ikke gå ut fra at det vil bli gitt utsettelse i perioden klagen blir behandlet.

§ 8-1. Kontroll

Beredskapsmyndigheten fører kontroll med at bestemmelser gitt i eller i medhold av denne forskriften overholdes.

Virksomheten skal medvirke til gjennomføring av kontroll. Dette omfatter blant annet å fremskaffe dokumentasjon og opplysninger som er nødvendige for å gjennomføre kontroll, og gi beredskapsmyndigheten adgang etter energiloven § 9-5 annet ledd.

8.1.1 Hensikten med bestemmelsen

Formålet med NVEs tilsyn er gjennom kontroll og bruk av reaksjoner å bidra til å sikre at virksomhetene overholder kravene gitt i eller i medhold av beredskapsforskriften.

8.1.2 Nærmere om ulike metoder for kontroll

Kontrollmyndigheten omfatter både bestemmelsene i beredskapsforskriften og vedtak truffet i medhold av forskriften. Beredskapsmyndighetens kontrollvirksomhet må ses i sammenheng med plikten til internkontroll etter § 2-10.

KBO-enhetene har plikt til å medvirke til at beredskapsmyndigheten kan gjennomføre tilsyn. Den særlige opplysningsplikten etter denne bestemmelsen suppleres av den generelle opplysningsplikten etter *energiloven* § 10-1, tredje ledd.

NVE benytter følgende metoder for å føre tilsyn med virksomheter underlagt denne forskriften:

1. Revisjon

Revisjon er en uavhengig, systematisk og dokumentert gjennomgang av hele eller deler av en virksomhet for å kontrollere og bedømme om en virksomhet oppfyller krav gitt i eller i medhold av denne beredskapsforskriften.

2. Inspeksjon

Inspeksjon er en uavhengig og dokumentert gjennomgang av hele eller deler av en virksomhet for å kontrollere og bedømme om virksomheten oppfyller krav gitt i eller i medhold av beredskapsforskriften.

3. Andre kontrollaktiviteter

Andre kontrollaktiviteter er ulike former for undersøkelser som gjennomføres i enkelttilfeller eller som aksjoner/kampanjer for å kontrollere og bedømme om virksomheten oppfyller krav gitt i eller i medhold av beredskapsforskriften.

- a. Sammenstilling av informasjon. Dette kan være gjennomgang av informasjon som virksomheten har offentliggjort på Internett eller på annen måte. Det kan også være sammenstilling av fagdatabaser og innrapporterte data, både til NVE og til andre myndigheter.
- b. Skriftlige tilsynsundersøkelser. Dette kan være skjema som sendes til en bestemt gruppe virksomheter eller til alle, og som inneholder spørsmål om hvordan utvalgte bestemmelser i forskriften etterleves.

Tilsyn kan benyttes overfor alle virksomheter innenfor forskriftens virkeområde. Tilsyn med virksomhetene kan gjennomføres i planleggings- utbyggings- drifts- og avviklingsfasen. Tilsyn kan gjelde hele eller deler av virksomheten, og rette seg mot overordnede systemer, spesifikke krav eller konkrete problemstillinger. Tilsyn kan være varslet eller uanmeldt. Tilsyn kan utføres på eget initiativ eller på oppfordring fra andre.

Kontroll og tilsyn kan resultere i avvik eller anmerkning. Avvik er brudd på krav gitt i eller i medhold av beredskapsforskriften. Anmerkning er en påpekning av forhold som bør vurderes nærmere av virksomheten, men som ikke er brudd på krav gitt i eller i medhold av beredskapsforskriften.

§ 8-2. Pålegg

Beredskapsmyndigheten kan gi de pålegg som er nødvendige for gjennomføring av bestemmelser gitt i eller i medhold av denne forskrift.

8.2.1 Hensikten med bestemmelsen

Bestemmelsen klargjør at beredskapsmyndigheten har hjemmel for å gi pålegg. Pålegg kan gis både når det gjelder gjennomføring av bestemmelser i beredskapsforskriften og vedtak truffet i medhold av forskriften.

8.2.2 Nærmere om pålegg

Pålegg kan for eksempel være pålegg om retting, det vil si endringer som virksomheten kan pålegges å gjennomføre for at tiltaket eller virksomheten skal bli i tråd med regelverket.

NVE vil gi pålegg om retting i tilfeller hvor det er mulig å gjenopprette lovlig tilstand, slik at man får understreket kravene som følger av forskriften. Retting er for eksempel aktuelt der et klassifisert anlegg ikke oppfyller kravene til fysisk sikring, eller hvor beredskapsplanverket ikke oppfyller kravene i forskriften.

NVE vil alltid sette en frist for retting. Fristen skal settes slik at virksomheten har en reell mulighet til å rette på forholdet innen fristen. For eksempel skal NVE ta hensyn til

årstiden og praktiske forhold som for eksempel leveringstid på anleggsdeler. Hvis fristen ikke overholdes, kan det gis vedtak om tvangsmulkt fram til retting har skjedd, hvis dette ikke allerede er gjort samtidig med at vedtak om retting ble gitt.

Pålegg om retting er et enkeltvedtak. Et pålegg om retting har umiddelbar virkning, slik at rettingen skal skje innenfor den angitte fristen. Men etter *forvaltningsloven* § 42 kan det bestemmes at en eventuell klage til Olje- og energidepartementet gis oppsettende virkning, slik at pålegget ikke effektueres før klagen er behandlet. Dette må vurderes konkret i det enkelte tilfellet.

§ 8-3. Dispensasjon

Beredskapsmyndigheten kan i særlige tilfeller gi dispensasjon fra bestemmelser gitt i eller i medhold av denne forskrift.

8.3.1 Hensikten med bestemmelsen

Det kan forekomme spesielle forhold der det kan være rimelig å gi dispensasjon fra reglene i denne forskriften. Bestemmelsen gir NVE myndighet til å beslutte at det kan gis dispensasjon gjennom bruk av enkeltvedtak.

8.3.2 Nærmere om dispensasjon

Det er ikke mulig å gi generell veiledning for hvilke særlige tilfeller det vil bli gitt dispensasjon. Behovet for å fravike forskriftens krav må vurderes fra sak til sak. Det kan settes vilkår for en dispensasjon. Økonomiske betraktninger vil i svært liten grad gi grunnlag for dispensasjon. Bestemmelsen vil bli praktisert strengt.

§ 8-4. Tvangsmulkt

Ved overtredelse av bestemmelser gitt i eller i medhold av denne forskrift, kan beredskapsmyndigheten ilegge tvangsmulkt i medhold av energiloven § 10-3.

8.4.1 Hensikten med bestemmelsen

Bestemmelsen klargjør beredskapsmyndighetens myndighet til å bruke tvangsmulkt som reaksjon med det formål å framtvinge lovlig tilstand. Henvisningen til *energiloven* § 10-3 angir at bruken av tvangsmulkt må skje på de vilkår som følger av denne bestemmelsen.

8.4.1 Nærmere om tvangsmulkt

Vedtak om tvangsmulkt er et enkeltvedtak. Det medfører at reglene i *forvaltningsloven* kapittel IV-VI om blant annet varsel, utredningsplikt, begrunnelse og klagerett gjelder.

Formålet med tvangsmulkt er å tvinge enheten til å oppfylle kravene, herunder at lovlig tilstand gjenopprettes. Tvangsmulkt er derfor i utpreget grad rettet framover, siden hensikten er at den skal motivere mottakeren til å innrette seg lovlig så raskt som mulig.

NVE bruker tvangsmulkt når plikter som er gitt i eller i medhold av denne forskriften, ikke blir oppfylt. NVE kan gi pålegg (vedtak) om forhold som er i strid med regelverket, og hvis ikke vedtaket er gjennomført innen den fastsatte fristen, kan NVE følge opp med tvangsmulkt.

Tvangsmulkt fastsettes enten som en løpende mulkt eller som et engangsbeløp.

§ 8-5. Overtredelsesgebyr

Ved overtredelse av bestemmelsene i kapittel 2 til 7, inkludert vedleggene til kapittel 5, og vedtak truffet i medhold av § 8-3 kan det ilegges overtredelsesgebyr i medhold av energiloven §§ 10-7 og 10-8.

8.5.1 Hensikten med bestemmelsen

Hensikten med overtredelsesgebyr er å sikre etterlevelse av regelverket.

8.5.2 Nærmere om overtredelsesgebyr

Overtredelsesgebyr er en sanksjon som kan benyttes mot brudd på de av beredskapsforskriftens bestemmelser som er særskilt nevnt i bestemmelsen, i henhold til *energiloven* §§ 10-7 og 10-8. I tillegg er det adgang til å ilegge overtredelsesgebyr for brudd på *energiloven* kapittel 9.

Overtredelsesgebyr er en administrativ sanksjon som skiller seg fra straff ved at det er forvaltningen (NVE) og ikke domstolene/politiet som ilegger reaksjonen.

Overtredelsesgebyr medfører at enheten blir pålagt å betale et pengebeløp som sanksjon for en overtredelse. Overtredelsesgebyr er altså tilbakeskuende, det vil si en reaksjon på noe som har skjedd.

Vedtak om overtredelsesgebyr er et enkeltvedtak. For å treffe vedtak om å ilegge overtredelsesgebyr kreves det:

- At den handlingen som er begått, rent objektivt rammes av pliktregler som er nevnt i denne bestemmelsen.
- At det foreligger subjektiv skyld, det vil si enten i form av forsett eller uaktsomhet
- At NVE finner at overtredelsesgebyr bør ilegges.

At handlingen rent objektivt rammes av en pliktregel, betyr at det rent faktisk kan konstateres at en plikt er overtrådt. For eksempel vil det klart rammes av rapporteringsplikten i § 2-6 dersom en enhet unnlater å rapportere om et havari av et klassifisert anlegg. Siden denne bestemmelsen er nevnt i § 8-5, kan overtredelse bli sanksjonert med overtredelsesgebyr.

På energilovens område vil de fleste overtredelser begås av foretak. For at et foretak skal kunne ilegges gebyr, må det også foreligge skyld, i form av forsett eller uaktsomhet, hos enkeltperson(er) som handler på vegne av foretaket. For uoverlagte uhell og særlige omstendigheter som ikke er under menneskelig kontroll, som for eksempel naturkatastrofer, kan ikke foretak ilegges overtredelsesgebyr.

Vurderingen av om overtredelsesgebyr bør ilegges foretak skjer med utgangspunkt i de momentene som er nevnt i *energiloven* § 10-8 om overtredelsens grovhet mv.

Overtredelsesgebyrets størrelse fastsettes av NVE etter en skjønnsmessig og konkret vurdering. Blant annet skal det ved utmåling av overtredelsesgebyr tas hensyn til at overtredelsen:

- Ikke skal lønne seg.
- Skal være merkbar.
- Gebyrets størrelse vil kunne avhenge av selskapets økonomiske stilling.

§ 8-6. Straff

Overtredelse av bestemmelsene i kapittel 2-8, inkludert vedleggene til kapittel 5, kan straffes med bøter eller fengsel i medhold av energiloven § 10-5.

8.6.1 Hensikten med bestemmelsen

Hensikten med overtredelsesgebyr er å sikre etterlevelse av regelverket. Brudd på de særskilt nevnte bestemmelsene kan medføre straff.

8.6.2 Nærmere om straff

Henvisningen til *energiloven* § 10-5 angir at illeggelse av straff må skje på de vilkårene som følger av denne bestemmelsen. Bestemmelsen gir ikke beredskapsmyndigheten hjemmel til å straffe. Det vil være domstolene som legger straffeansvar etter at påtalemyndigheten har tatt ut tiltale.

Bestemmelsen bør ses i sammenheng med reglene om overtredelsesgebyr og tvangsmulkt, som gir forvaltningen flere alternative sanksjonsmuligheter. Straff er én av disse. På samme måte som for overtredelsesgebyr, følger det av forskriften hvilke bestemmelser dette er relevant for.

§ 8-7. Gebyr til beredskapsmyndigheten

Til dekning av beredskapsmyndighetens utgifter til arbeidet med energiforsyningsberedskap innkreves et årlig gebyr.

Gebyret fastsettes for det enkelte kraftselskap på grunnlag av installert ytelse i kraftverk, transformatorstasjoner og nettstasjoner pr. 1. januar det år gebyret beregnes for. Satsene skal reguleres slik at de samlede gebyrer tilsvarer de faktiske utgifter beredskapsmyndigheten har med beredskapsarbeidet.

8.7.1 Hensikten med bestemmelsen

Gebyret finansierer beredskapsmyndighetens arbeid.

8.7.2 Nærmere om beredskapsgebyret

Beredskapsmyndigheten (NVE) krever inn gebyr med hjemmel i *energiloven* § 9-6, for å finansiere sine utgifter til beredskapsarbeidet i energiforsyningen. Beregningsmåten for gebyret vil være den samme som før (etter tidligere *energilovforskriften* § 8-6).

§ 8-8. Ikrafttreden

Denne forskriften trer i kraft 1. januar 2013. Fra samme tid oppheves forskrift 16. desember 2002 nr. 1606 om beredskap i kraftforsyningen.

8.8.1 Hensikten med bestemmelsen

Bestemmelsen angir at forskriften trådte i kraft fra 1. januar 2013. Det innebærer at alle krav som følger av forskriften gjelder fullt ut og vil bli håndhevet fra samme tidspunkt, med mindre det gjelder et område som er omfattet av overgangsbestemmelsen (§ 8-9).

Bestemmelsen klargjør også at beredskapsforskriften fra 2002 ble opphevet fra samme tidspunkt.

8.8.2 Nærmere om ikrafttredelse

Etter NVEs vurdering viderefører ny forskrift i all hovedsak dagens krav etter dagens beredskapsforskrift, enkeltvedtak med hjemmel i denne forskrift og tidligere enkeltvedtak. På denne bakgrunn legger NVE til grunn at også anlegg som fikk konsesjon før 01.01.2013, men som blir idriftsatt etter at forskriften trådte i kraft, også skal oppfylle kravene etter ny forskrift. For kravene til sikringstiltak etter kapittel 5, mener NVE det er behov for en viss overgangsperiode. Vi viser til veiledning til § 8-9 nedenfor.

§ 8-9. Forholdet til eldre vedtak om klassifisering og overgangsregler

Vedtak om sikring eller andre vedtak i medhold av forskrift 16. desember 2002 nr. 1606 om beredskap i kraftforsyningen truffet etter 1. januar 2003 og før 1. januar 2013 står fortsatt ved lag inntil de blir endret eller opphevet i medhold av denne forskrift.

Anlegg som er idriftsatt før 1. januar 2013, og som ikke er omfattet av vedtak omtalt i første ledd, klassifiseres etter denne forskrift, men slik at sikringstiltak etter kapittel 5 kan tilpasses bygningsteknisk utforming og tidligere pålegg om fysisk sikring. Ved vesentlig ombygging eller utvidelse vil kravene etter kapittel 5 gjelde fullt ut for den del av anlegget som endres.

Vedtak om beredskapsmessige forhold til kraftforsyningen om annet enn klassifisering og sikringstiltak truffet før 1. januar 2003, og som ikke er erstattet av senere vedtak eller forskrifter står ved lag så langt de passer inntil de blir endret eller opphevet i medhold av denne forskrift.

Alle anlegg som er idriftsatt etter 1. januar 2013 skal klassifiseres og sikres etter denne forskrift. Dette gjelder selv om de har fått konsesjon før 2013. For disse anleggene gjelder en overgangsperiode på 2 år. Beredskapsmyndigheten kan gi én dispensasjon fra dette. Slik dispensasjon kan kun gis én gang for hvert anlegg for en periode på inntil 2 år.

8.1.9 Hensikten med bestemmelsen

Bestemmelsen beskriver hvordan denne forskriften skal forstås i lys av tidligere regelverk og tidligere vedtak. Etter *energiloven* kapittel 9 Beredskap kan myndighetene stille krav om å gjennomføre nye eller endrede tiltak ved både nye og eksisterende energiforsyningsanlegg, uavhengig av tidligere pålegg. Overgangsbestemmelsen fastsetter hvordan forskriften normalt vil bli praktisert ved eksisterende anlegg, og dermed også en pekepinne for NVEs tilsyn.

8.9.2 Nærmere om forholdet til BfK fra 2002

Første ledd angir at vedtak om sikring truffet etter BfK, fortsatt står ved lag. Den nåværende ordningen med klassifisering av anlegg ved enkeltvedtak legges om slik at klassifisering nå vil følge direkte av forskriften. Det er derfor behov for å presisere at vedtakene etter den gamle beredskapsforskriften (BfK) fra 2002 fortsatt skal gjelde. Første ledd omfatter ikke vedtak om klassifisering og sikring som er truffet før BfK trådte i kraft 1. januar 2003.

Også andre vedtak står ved lag, for eksempel vedtak om rutiner for varsling av KBO eller vedtak om retting etter tilsyn. Vedtak som NVE har truffet etter gjennomførte

beredskapstilsyn, står ved lag med mindre vedtaket omhandler krav som ikke er videreført i bfe.

Formuleringen ”inntil de blir endret eller opphevet” henspiller på § 5-7, og adgangen til å fatte enkeltvedtak om klassifisering og sikringstiltak.

8.9.3 Anlegg uten enkeltvedtak etter BfK

Annet ledd omhandler eldre anlegg som ikke er omfattet av enkeltvedtak etter beredskapsforskriften av 2002 i perioden 01.01.2003 til 01.01.2013. Reglene om sikring og klassifisering etter denne forskrift med presiseringene nedenfor gjelder enten det for slike eldre anlegg er truffet tidligere vedtak om sikring og klassifisering i medhold av regelverk som gjaldt før beredskapsforskriften av 2002 eller ikke. Mange eksisterende anlegg vil være av eldre dato, noe anleggene kan bære preg av. Samtidig forventer NVE at mange eldre anlegg vil utvides eller ombygges i årene framover. På grunn av anleggets utforming vil det i mange tilfeller ikke være hensiktsmessig å gjennomføre sikringstiltak for eksisterende anlegg som helt ut fyller krav etter denne forskriften.

Overgangsbestemmelsen innebærer at det kan tas hensyn til anleggenes alder og i hvilken grad de oppfyller tidligere pålagte sikringstiltak ved vurderingen av om et anlegg oppfyller krav til sikring. Utgangspunktet er likevel at tidligere pålagte sikringstiltak er gjennomført. Dette gjelder selv om disse ikke er hensiktsmessige etter dagens forhold, eller at de ikke fullt ut oppfyller dagens forskrift.

Normalt krever ikke NVE at det skal utføres sikringstiltak som innebærer vesentlige endringer i planløsninger, bygningsmasse eller hvordan de elektriske høyspenningsanleggene er arrangert, og som medfører store ombygginger av eksisterende anlegg. Annet ledd gir ikke grunnlag for dispensasjon fra tidligere pålagte tiltak som ikke er gjennomført.

Dette gjelder likevel ikke særlig viktige anlegg eller særlig dårlig sikrede anlegg.

Dersom vedtak om klassifisering av anlegg fra før 01.01.2003 er truffet på bakgrunn av en bredere vurdering enn kriteriene som framgår av denne forskrift (§ 5-2), og den enkelte virksomhet opplever en eventuell oppklassifisering av anlegg som urimelig, forventes det at virksomheten henvender seg til NVE. Dersom oppklassifisering må anses urimelig, tar NVE sikte på å gi disse virksomhetene en særskilt vurdering av disse anleggenes klasse etter § 5-7.

8.9.4 Eldre vedtak om tilskudd til reservemateriell

Tredje ledd tar særlig sikte på vedtak som tidligere er truffet om tilskudd til og forvaltning av reservemateriell, og innebærer at vilkårene om forvaltning av reservemateriellet står ved lag. Bestemmelsen gjelder også eventuelle andre vedtak. Endret ordlyd, jf høringsdokumentet, er kun ment som en språklig endring.

8.9.5 Anlegg som idriftssettes etter 01.01.2013

Fjerde ledd innebærer at beredskapsmyndigheten ikke vil ferdigbehandle søknader om klassifisering mottatt før ikrafttreddelsen av denne forskriften. Dette skyldes at klassifisering etter revidert forskrift som hovedregel ikke lenger vil bli besluttet ved enkeltvedtak, men vil følge direkte av forskriften. Dersom et anlegg bør klassifiseres i en

annen klasse enn det som framgår etter reglene i denne forskriften, vil det være adgang til dette etter reglene i § 5-7.

Fjerde ledd omfatter også anlegg som har fått konsesjon før 01.01.2013, men som vil bli idriftssatt etter at denne forskriften er trådt i kraft. NVE finner det sannsynlig at alle anlegg som Statkraft har fått konsesjon til er omfattet av meldeplikten etter dagens beredskapsforskrift, hvor praksis er å gi klasse og pålegg om sikringstiltak gjennom enkeltvedtak. I de tilfeller hvor endring av forskriften innebærer strengere krav til sikring enn det som ble lagt til grunn for planlegging og utførelse av et anlegg (jf også *energilovforskriften* § 3-5 bokstav c og 5-3 bokstav c som ikke er idriftssatt ved ikrafttredelse av denne forskriften, kan anleggets samfunnsmessige betydning og planlagte sikringstiltak tillegges betydning som bakgrunn for enkeltvedtak for disse anleggene etter § 5-7.

9. Litteratur

Almindelig borgerlig Straffelov (Straffeloven), LOV-1902-05-22-10.

Besøksrestriksjoner og adgangskontroll ved kraftanlegg. Presisering av bestemmelser i beredskapsforskrift for kraftforsyningen, NVE, enkeltvedtak av 29.06.2006.

BfK (2002), *Forskrift om beredskap i kraftforsyningen*. Forskriften ble opphevet 01.01.2013.

Delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat, FOR 2012-12-07 nr 1156.

Delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat, FOR 2012-12-07 nr 1156.

Direktiv for øvelser ved m.m. ved kraftforsyningsanlegg. Fastsatt av Elektrisitetstilsynet og Norges vassdrags- og energiverk med virkning fra 1. september 1993.

Eksempelsamling Risiko- og sårbarhetsanalyser for kraftforsyningen. NVE Rapport 18-2012.

Forsikringsselskapenes Godkjennelsesnemnd (FG): *Krav til system og enkeltkomponenter for elektronisk avlåsning i beskyttelsesklassene B1, B2 og B3. Informasjon og Krav*, 2010.

Forskrift for oljerasjonering ved beredskap og krig, FOR 1983-12-15 nr 2142.

Forskrift for sivil transportberedskap, FOR 2005-06-14-548.

Forskrift om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett (autorisasjonsforskriften), FOR-2005-03-04-200.

Forskrift om behandling av personopplysninger (personopplysningsforskriften), FOR-2000-12-15-1265.

Forskrift om brannforebyggende tiltak og tilsyn (forebyggendeforskriften), fastsatt av Direktoratet for samfunnssikkerhet og beredskap (DSB) 26. juni 2002.

Forskrift om elektriske forsyningsanlegg (FEF), FOR-2005-12-20-1626 med veiledning fastsatt av DSB.

Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften), FOR-2004-02-16-401.

Forskrift om energiutredninger, FOR 2012-12-07 nr 1158.

Forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff, samt utstyr og anlegg som benyttes ved håndteringen, FOR-2009-06-08-602.

Forskrift om innkjøp i forsyningssektorene, FOR 2006-04-07-403.

Forskrift om kommunal beredskapsplikt, FOR-2011-08-22-894.

Forskrift om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften), FOR 2011-03-10-263.

Forskrift om kvalifikasjoner for elektrofagfolk, FOR-1993-12-14-1133.

Forskrift om merking av luftfartshinder (BSL E 2-2), FOR 2002-12-03 nr 1384.

Forskrift om militære rekvisisjoner, FOR 1999-09-17 nr 1012.

Forskrift om objektsikkerhet, FOR-2010-10-22-1362.

Forskrift om oljerasjonering ved oljeforsyningskriser i fredstid, FOR 1983-08-01-2141.

Forskrift om planlegging og gjennomføring av rekvisisjon av kraft og tvangsmessige leveringsinnskrenkninger ved kraftrasjonering, FOR 2001-12-17 nr 1421.

Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskriften), FOR 1990-12-07 nr 959.

Forskrift om rapportering og registrering av luftfartshindre (BSL E 2-1), FOR 2003-04-14 nr 514.

Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg (FSE), FOR-2006-04-28-458.

Forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften), FOR-2009-12-18-1600.

Forskrift om systemansvaret i kraftsystemet (FoS), FOR-2002-05-07-448.

Forskrift om tekniske krav til byggverk (Byggteknisk forskrift – TEK 10), FOR-2010-03-26-489.

Forskrift om tilfluktsrom, FOR-1995-03-15-254.

Forskrift om utleie av vannkraftanlegg, FOR-2010-06-25 nr 939.

Funksjonskrav i kraftsystemet (FIKS), Statnett SF 2012.

Håndbok for forberedt rekvirering av sivile kjøretøyer (TH 100-12), Forsvarets Logistikkorganisasjon, 1984.

Isstorm. Ising på kraftforsyningsnettet. NVE-rapport nr 44-2012.

Konsesjonshandsaming av vasskraftsakar. Rettleiar for utarbeiding av meldingar, konsekvensutgreiingar og søknader. NVE Rettleiar 3-2010.

Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven), LOV-2005-06-17-62.

Lov om behandling av personopplysninger (personopplysningsloven), LOV-2000-04-14-31.

Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), LOV-1967-02-10.

Lov om elektronisk kommunikasjon (ekomloven), LOV-2003-07-04-83.

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), LOV-1998-03-20-10.

Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven), LOV-2010-06-25-45.

Lov om militære rekvisisjoner, LOV 1951-06-29-19.

Lov om petroleumsvirksomhet (petroleumsloven), LOV-1996-11-29-72.

Lov om planlegging og byggesaksbehandling (plan- og bygningsloven - pbl.), LOV-2008-06-27-71.

Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven), LOV-1990-06-29-50.

Lov om rett til innsyn i dokument i offentlig verksemd (offentleglova), LOV-2006-05-19-16.

Lov om tilsyn med elektriske anlegg og elektrisk utstyr (el-tilsynsloven), LOV-1929-05-24-4.

Lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver (brann- og eksplosjonsvernloven), LOV-2002-06-14-20.

Lynstudien. Klimaendringenes betydning for forekomsten av lyn og tilpasningsbehov i kraftforsyningen. NVE-rapport 6-2011.

Norsk Elektroteknisk Komite (NEK), 445:2009 *Luftledninger over 1 kV*.

Norsk Elektroteknisk Komite (NEK), NEK 400:2010 *Elektriske lavspenningsinstallasjoner*.

Norsk Elektroteknisk Komite (NEK), NEK 440:2011 *Stasjonsanlegg over 1 kV*.

Reparasjonsberedskap i sentral- og regionalnettet og tilknyttede kraftstasjoner. Prosjektrapport med tiltak for god reparasjonsberedskap. NVE, 2011. Rapporten er tilgjengelig på www.nve.no.

Skytjenester i energiforsyningen – en forstudie, Deloitte, 2013. Forstudien kan lastes ned fra www.nve.no, eller fås ved å kontakte NVE, seksjon for beredskap.

Statens vegvesen, omregistrering av kjøretøyer, kodehefte autosys. www.vegvesen.no.

Temaveiledning – brannvern i kraftforsyningen, Direktoratet for samfunnssikkerhet og beredskap (DSB) og Norges vassdrags- og energidirektorat (NVE), november 2003.

Trær til besvær. Lærdommer om skogrydding i etterkant av ekstremværet Dagmar. Nve-rapport nr. 45-2012.

Utforming av konsesjonssøknad for fjernvarmeanlegg. NVE Veileder 2-2011.

Veileder for utforming av melding om bygging av kraftoverføringsanlegg. Meldinger etter plan- og bygningsloven kap. 14 og tilhørende forskrift om konsekvensutredninger. NVE, sist revidert 18.05.2010.

Veileder for utforming av søknad om anleggskonsesjon for kraftoverføringsanlegg. NVE, sist revidert 24.01.2011, ny versjon vil foreligge i løpet av 2013.

Veileder i utforming av konsesjonssøknader for vindkraftverk ≤ 10 MW. NVE:
www.nve.no.

Veiledning forskrift om elektriske forsyningsanlegg, fastsatt av DSB i 2006.

Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. NVE-Veileder 2-2010.

10. Forskriftstekst

Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften)

Fastsatt av Norges- vassdrags- og energidirektorat 7. desember 2012 med hjemmel i lov 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) §§ 9-1, 9-2 og 9-3 og forskrift 7. desember 1990 nr. 959 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovforskriften) § 9-1, gitt med hjemmel i energiloven § 10-6.

Kapittel 1. Innledende bestemmelser

§ 1-1. Formål

Innenfor formålene i energiloven § 1-2, skal forskriften sikre at energiforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene.

§ 1-2. Virkeområde

Forskriften gjelder forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring og fordeling av elektrisk energi eller fjernvarme.

§ 1-3. Hvem forskriften er rettet mot

Forskriften gjelder for de virksomheter som etter § 3-3 er enheter i Kraftforsyningens beredskapsorganisasjon (KBO). Forskriften gjelder også for de virksomheter som etter vedtak blir KBO-enheter.

Forskriftens kapittel 5 gjelder for de virksomheter som eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme.

Forskriftens § 6-2 om taushetsplikt for sensitiv informasjon gjelder for enhver.

Kapittel 2. Generelle krav

§ 2-1. Ansvar

Leder for virksomhet som er omfattet av denne forskrift har ansvar for at:

- a. Virksomheten har en organisasjon med de funksjoner som kreves i denne forskrift, og at det er etablert klare ansvars- og myndighetsforhold.
- b. Virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift.
- c. Kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift oppfylles.

d. Internkontroll etableres og praktiseres.

§ 2-2. Organisasjon og funksjon

Virksomhet som omfattes av denne forskrift skal ha følgende funksjoner:

a. Beredskapsleder. Denne utpekes av leder for virksomheten og skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet.

b. Beredskapskoordinator. Denne skal være administrativt kontaktpunkt til beredskapsmyndigheten.

c. IKT-sikkerhetskoordinator. Denne skal være faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet.

§ 2-3. Beredskapsplikt

Virksomhet som er omfattet av denne forskrift, skal sørge for effektiv sikring og beredskap, og skal iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner i samsvar med energiloven § 9-2 første ledd.

§ 2-4. Risiko og sårbarhetsanalyse

Alle KBO-enheter skal gjennomføre risiko- og sårbarhetsanalyser knyttet til ekstraordinære forhold. Analysene skal ha et slikt omfang at enheten kan identifisere risiko og sårbarhet ved alle funksjoner, anlegg og tiltak av betydning for å oppfylle kravene i forskriften. Analysene skal minimum gjennomgå årlig og oppdateres ved behov.

§ 2-5. Beredskapsplanlegging

Alle KBO-enheter skal ha et oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang. Planverket skal bygge på risiko- og sårbarhetsanalyser og skal omfatte alle beredskapstiltak etter denne forskriften.

Beredskapsplanleggingen skal blant annet omfatte forberedelser og tiltak det kan bli nødvendig å iverksette ved store ulykker, vesentlige skader, trusselsituasjoner, rasjonering og andre ekstraordinære situasjoner som kan påvirke energiforsynings drift og sikkerhet. Beredskapsplanverket skal, innenfor rammene av kapittel 6 om informasjonssikkerhet, samordnes med berørte myndigheter og andre relevante virksomheter, deriblant andre KBO-enheter.

§ 2-6. Varsling og rapportering

Alle KBO-enheter skal uten ugrunnet opphold varsle beredskapsmyndigheten om ekstraordinære situasjoner. Varslet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson.

Alle KBO-enheter skal uten ugrunnet opphold og senest innen tre uker skriftlig innrapportere følgende uønskede hendelser til beredskapsmyndigheten:

a. Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS).

b. Innbrudd, hærverk, sabotasje eller andre kriminelle handlinger, eller forsøk på dette.

- c. Mistenkelig adferd ved viktige anlegg av betydning for energiforsyningen.
- d. Situasjoner hvor sensitiv informasjon om kraftforsyningen er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette.
- e. Avbrudd i distribusjon av elektrisitet i mer enn to timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere.
- f. Avbrudd i fjernvarmeforsyningen i mer enn 12 timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere.
- g. Større havarier i sentral- og regionalnettet.
- h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer.

Beredskapsmyndigheten kan kreve rapportering av andre tilfeller av uønskede hendelser enn de som er nevnt i første og annet ledd.

Beredskapsmyndigheten kan også pålegge virksomheter som eier eller driver anlegg eller system, som er eller kan bli av vesentlig betydning for produksjon, omforming, omsetning eller fordeling av elektrisk energi og fjernvarme, å rapportere uønskede hendelser i samsvar med andre ledd.

§ 2-7. Øvelser

Alle KBO-enheter skal gjennomføre øvelser med slikt innhold og omfang at enheten vedlikeholder og utvikler sin kompetanse til å håndtere alle aktuelle ekstraordinære situasjoner. Virksomheten skal ha en flerårig øvelsesplan og gjennomføre minimum én årlig øvelse.

§ 2-8. Informasjonsberedskap

Alle KBO-enheter skal ha en informasjonsplan og en effektiv informasjonsberedskap i ekstraordinære situasjoner. Dette skal blant annet omfatte informasjon internt i enheten, til berørte myndigheter, samfunnskritiske virksomheter, andre relevante KBO-enheter, publikum og media, samt råd til kunder. Informasjonsplanen skal inngå som del av beredskapsplanverket, øves jevnlig og evalueres.

§ 2-9. Evaluering

Alle KBO-enheter skal etter ekstraordinære situasjoner og øvelser gjennomføre en evaluering. Evalueringen skal brukes som grunnlag for at virksomhetens beredskapskompetanse utvikles, at risiko- og sårbarhetsanalyser og beredskapsplaner oppdateres, og at det gjennomføres konkrete beredskapstiltak for anlegg, drift, gjenoppretting og øvrige tiltak som oppfyller kravene i denne forskriften.

§ 2-10. Internkontrollsystem

Alle KBO-enheter skal ha et internkontrollsystem som dokumenterer at det er etablert en systematikk for å sikre etterlevelse av kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c og bestemmelser gitt i eller i medhold av denne forskrift.

Internkontrollsystemet skal gjenspeile faktisk tilstand, og skal inneholde dokumentasjon for at alle tiltak etter kravene i første ledd er på plass og fungerer etter sin hensikt.

Internkontrollsystemet skal være tilrettelagt for gjennomføring av tilsyn i samsvar med de krav som er stilt.

Kapittel 3. Kraftforsyningens beredskapsorganisasjon (KBO)

§ 3-1. Organisering av KBO

Kraftforsyningens beredskapsorganisasjon består av KBO-enhetene, kraftforsyningens distriktssjefer (KDS) og beredskapsmyndigheten, samt kraftforsyningens sentrale ledelse (KSL) når denne trer i kraft, jf § 3-5.

§ 3-2. Beredskapsmyndigheten

Beredskapsmyndigheten skal i samsvar med energiloven § 9-1 tredje ledd utpeke den samlede ledelse i KBO og samordne beredskapsarbeidet.

§ 3-3. KBO-enheter

KBO-enheter er de virksomheter som eier eller driver anlegg og som har konsesjon etter energiloven §§ 3-1, 3-2 eller 5-1, og som i medhold av § 5-2 eller § 5-7 er klassifisert etter denne forskrift.

Beredskapsmyndigheten kan ved enkeltvedtak bestemme at også andre virksomheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, skal være KBO-enheter.

§ 3-4. Ansvar og oppgaver for KBO-enhetene

KBO-enhetene har ansvar for å utføre alle de oppgaver og plikter som følger av energiloven kap 9 og bestemmelser gitt eller i medhold av denne forskrift, herunder planlegging og håndtering av ekstraordinære situasjoner og gjenoppretting av normal situasjon.

Alle KBO-enheter skal sørge for nødvendig kontakt og samordning med tilgrensende virksomheter og aktuelle kraftforsyningens distriktssjefer.

Beredskapsmyndigheten kan pålegge KBO-enheter eller KBO å utføre oppgaver i medhold av energiloven § 9-1 fjerde ledd.

§ 3-5. Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig

KBO-enheter eller KBO kan pålegges oppgaver under beredskap og i krig i samsvar med energiloven § 9-1 femte ledd og etter at beredskapsmyndigheten ved vedtak har konstatert at det anses nødvendig.

Departementet kan under beredskap og krig underlegge energiforsyningen KBO. Energiforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves. Beredskapsmyndigheten kan instruere kraftforsyningens distriktssjefer og KBO-enheter.

I slike situasjoner overtar kraftforsyningens sentrale ledelse (KSL), bestående av beredskapsmyndigheten med deltakelse fra Statnett SF, ledelsen av KBO. Statnett SF skal

i slike situasjoner være KSLs utøvende organ for regulering av produksjon, omforming, overføring og fordeling av elektrisk energi.

Statnett SF må innrette sin organisasjon slik at virksomheten har regionale representanter med myndighet til å iverksette pålegg og gjennomføre de tiltak som kreves i en ekstraordinær situasjon, inkludert løpende kontakt med kraftforsyningens distriktssjefer.

§ 3-6. Ansvar og oppgaver for kraftforsyningens distriktssjefer

Beredskapsmyndigheten beslutter inndeling av distrikter og utpeker kraftforsyningens distriktssjefer med stedfortredere.

Kraftforsyningens distriktssjefer (KDS) skal bidra til å tilrettelegge for hensiktsmessig samarbeid om forebygging og håndtering av ekstraordinære situasjoner. Oppgaver for KDS kan reguleres gjennom avtaler mellom beredskapsmyndigheten og den person som er utpekt som KDS og i årlige forventningsbrev. Fullmakt til vedtak kan delegeres fra beredskapsmyndigheten til KDS.

§ 3-7. Fritaksordninger

Etter søknad fra en KBO-enhet kan personell som er viktig for å opprettholde driften av energiforsyningen i krig, få utsettelse eller fritak for fremmøte i Forsvaret ved mobilisering. Etter søknad fra en KBO-enhet kan dette personellet også få fritak for tjeneste i sivilforsvaret og politireserven. Personell i KBO som er gitt utsettelse eller fritak for annen beredskapstjeneste får tjenesteplikt i KBO.

Kapittel 4. Ressurser og reparasjonsberedskap

§ 4-1. Reparasjonsberedskap

Alle KBO-enheter skal planlegge for og etablere en organisasjon med nødvendig personell, kompetanse, utholdenhet og ressurser til å holde driften gående, gjenopprette funksjon og gjennomføre oppgaver som kreves under alle ekstraordinære situasjoner på en sikker og effektiv måte.

Reparasjonsberedskapen skal dimensjoneres etter stedlige forhold og anleggenes tilstand og klasse. Så langt som det er samfunnsmessig rasjonelt, skal hensynet til liv og helse og annen samfunnskritisk virksomhet prioriteres ved gjenoppretting av funksjon.

§ 4-2. Kompetanse og personell

Alle KBO-enheter skal ha personell med nødvendig kompetanse som kreves for kunne håndtere ekstraordinære situasjoner på en sikker og effektiv måte.

Alle KBO-enheter skal dekke dette personellbehovet og ha tilgang på personell for å forsterke kapasiteten og holde driften gående i ekstraordinære situasjoner.

For å dekke kravet til kompetanse og personell skal det foreligge en plan som angir kompetansebehovet, og som omfatter eget og innleid personell.

§ 4-3. Drift i ekstraordinære situasjoner og gjenoppretting av funksjon

Alle KBO-enheter skal i ekstraordinære situasjoner drive de anlegg og den del av energiforsyningen enheten har ansvaret for, herunder driftskontrollfunksjoner, og gjenopprette nødvendige funksjoner i og etter ekstraordinære situasjoner.

§ 4-4. Materiell og utstyr

Alle KBO-enheter skal ha rask og sikker tilgang til reservemateriell og utstyr som trengs for å opprettholde energiforsyningen i ekstraordinære situasjoner, og for å gjenopprette funksjon.

Med reservemateriell menes materiell som kan erstatte komponenter som er nødvendige for drift av anlegg.

Med utstyr menes verktøy, maskiner, reparasjonsmateriell, komponenter til driftskontrollsystemet og annet som er nødvendig for å foreta reparasjoner, gjenoppretting eller om nødvendig iverksette midlertidige tiltak.

Ressursbehovet kan dekkes ved at KBO-enheten enten har dette selv, eller sikrer tilgang fra andre. Utstyr og ressurser skal holdes i forsvarlig stand og være tilgjengelig for KBO-enheten i ekstraordinære situasjoner.

§ 4-5. Transport

Alle KBO-enheter skal ha en tilstrekkelig transportberedskap for å håndtere ekstraordinære situasjoner, og evne til rask gjenoppretting av funksjon. Dette omfatter tilgang til transportmidler med nødvendig utstyr og personer som kan håndtere disse.

For utstyr med transportvekt over 70 tonn, eller med store ytre dimensjoner, skal det utarbeides detaljerte transportplaner.

KBO-enhetenes transportmidler og private transportmidler tilhørende energiforsyningens personell som det er tjenstlig behov for, skal om mulig søkes fritatt for forberedt rekvirering til Forsvaret med videre.

§ 4-6. Nasjonal tungtransportberedskap

Statnett SF skal ha en nasjonal tungtransportberedskap for å sikre at tunge komponenter av betydning for energiforsyningen kan transporteres på kort varsel. Statnett SF skal vedlikeholde og oppgradere transportmidler med utstyr, samt anskaffe nye ressurser ved behov.

Statnett SF kan benytte den virksomhet som er etablert for å ivareta ansvar for tungtransportberedskap etter første ledd, til å utføre virksomhet for andre på markedsmessige vilkår. Endringer i virksomheten skal forelegges beredskapsmyndigheten for godkjenning.

Den nasjonale tungtransportberedskapen skal gjelde for ekstraordinære situasjoner, samt under beredskap og i krig.

Beredskapsmyndigheten kan treffe vedtak om organisering, bruk og finansiering av nasjonal tungtransportberedskap.

§ 4-7. Samband

Alle KBO-enheter skal ha intern og ekstern sambandsberedskap for daglig drift, håndtering av ekstraordinære situasjoner og evne til rask gjenoppretting av nødvendige funksjoner for ledelse, drift og sikkerhet.

Kapittel 5. Klassifisering og sikringstiltak

§ 5-1. Sikringsplikt

Eier eller driver plikter å sikre anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende. Med anlegg menes her også bygg og andre ressurser omfattet av kapittel 4.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter anleggets eller systemets type, oppbygging og funksjon.

Alle anlegg m.m. som nevnt i første ledd skal holdes i funksjonsdyktig stand og skal så langt som mulig virke etter sin hensikt under ekstraordinære forhold.

Det skal særlig tas hensyn til ekstraordinære forhold som:

- uvær og annen naturgitt skade
- brann og eksplosjoner
- alvorlig teknisk svikt
- innbrudd, hærverk, sabotasje og andre kriminelle handlinger

§ 5-2. Klasser

Ved klassifisering av anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme benyttes klasse 1 til 3. Klasse 3 benyttes der betydningen for energiforsyningen er størst.

Koblingsanlegg, kraftledning, mufteanlegg, lokalkontrollanlegg og annet som funksjonelt er en del av en kraft-, transformator- eller omformerstasjon klassifiseres etter vedkommende stasjons klasse.

Denne bestemmelse omfatter ikke energianlegg for rene industriformål eller energianlegg som eies av en virksomhet som selv er eneste sluttbruker av energien fra anlegget.

Denne bestemmelse omfatter ikke midlertidige energianlegg eller midlertidige løsninger som del av energianlegg når det foreligger konkrete planer for utbygging eller oppgradering av spenningsnivå.

I ytelseskriteriene i denne bestemmelse medregnes ikke mobile komponenter som reserveaggregat eller beredskapstransformatorer, midlertidige plasserte transformatorer, generatortransformatorer, eller transformatorer for regulering og spesielle formål (fasekompensering, spoler og lignende). For transformatorer med flere funksjoner (viklinger) regnes høyeste ytelse av transformering mellom nettnivåer.

Klasse 1 omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 25 MVA.
- b. Transformatorstasjon med samlet hovedtransformatorytelse på minst 10 MVA.
- c. Omformerstasjon med samlet installert ytelse for omforming på minst 10 MVA.
- d. Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 30 kV.
- e. Kraftledning bygget for et spenningsnivå på minst 5 kV.
- f. Fjernvarmesentral med samlet installert ytelse på minst 50 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.
- g. Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til d og f.

Klasse 2 omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 100 MVA og kraftstasjoner på minst 100 MVA plassert i dagen.
- b. Transformatorstasjon med samlet hovedtransformatorytelse på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.
- c. Omformerstasjon med samlet installert ytelse for omforming på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.
- d. Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 100 kV.
- e. Kraftledning bygget for et spenningsnivå på minst 30 kV.
- f. Fjernvarmesentral med samlet installert ytelse på minst 150 MW. I ytelsen skal medregnes effekt i ekstern varmeleveranse.
- g. Driftskontrollsystem plassert i klasse 2 etter enkeltvedtak.

Klasse 3 omfatter:

- a. Kraftstasjon i fjell med samlet installert generatorytelse på minst 250 MVA.
- b. Transformatorstasjon med samlet hovedtransformatorytelse på mer enn 100 MVA og bygget for et høyeste spenningsnivå på minst 200 kV og transformering til sekundært spenningsnivå i nett på minst 30 kV.
- c. Selvstendig koblingsstasjon i kraftsystemet bygget for et spenningsnivå på minst 200 kV.
- d. Kraftledning bygget for et spenningsnivå på minst 200 kV.
- e. Driftskontrollsystem plassert i klasse 3 etter enkeltvedtak.

§ 5-3. Sikring av klassifiserte anlegg

Alle klassifiserte anlegg skal prosjekteres, plasseres, utføres, utrustes, sikres, driftes og holdes i slik stand at risiko for skade, havari og funksjonssvikt og andre uønskede hendelser og handlinger blir minst mulig.

§ 5-4. Sikringstiltak for klasse 1

Anlegg klassifisert i klasse 1 skal, i tillegg til kravene til sikring etter §§ 5-1 og 5-3, oppfylle følgende generelle krav til sikring:

1. Anlegget skal utføres etter krav til normalt sikringsnivå, som nærmere angitt i vedlegg 1.
2. Skader og funksjonstap skal oppdages innen rimelig tid.
3. Skader skal utbedres og anleggets funksjoner skal gjenopprettes uten ugrunnet opphold.

Anlegg klassifisert i klasse 1 skal også oppfylle særlige krav til sikring for sin klasse og anleggstype som fastsatt i vedlegg 1, jf vedlegg 4.

§ 5-5. Sikringstiltak for klasse 2

Anlegg klassifisert i klasse 2 skal, i tillegg til kravene til sikring etter §§ 5-1 og 5-3, oppfylle følgende generelle krav til sikring:

1. Anlegget skal utføres og utstyres etter middels høye krav til sikring, som nærmere angitt i vedlegg 2.
2. Tap av vitale funksjoner skal begrenses og etter eventuell skade skal anleggets funksjonalitet gjenopprettes uten ugrunnet opphold.

Anlegg klassifisert i klasse 2 skal også oppfylle særlige krav til sikring for sin klasse og anleggstype som fastsatt i vedlegg 2, jf vedlegg 4.

§ 5-6. Sikringstiltak for klasse 3

Anlegg klassifisert i klasse 3 skal, i tillegg til kravene til sikring etter §§ 5-1 og 5-3, oppfylle følgende generelle krav til sikring:

1. Anlegget skal utføres og utstyres etter høye krav til sikring, som nærmere angitt i vedlegg 3.
2. Vitale funksjoner skal opprettholdes i ekstraordinære situasjoner og anleggets funksjonalitet skal gjenopprettes uten ugrunnet opphold.

Anlegg klassifisert i klasse 3 skal også oppfylle særlige krav til sikring for sin klasse og anleggstype som fastsatt i vedlegg 3, jf vedlegg 4.

§ 5-7. Vedtak om sikring eller klasse

Beredskapsmyndigheten kan treffe vedtak om andre eller ytterligere sikringstiltak i medhold av energiloven § 9-2 annet, jf tredje ledd. Ved vedtak skal det tas hensyn til anleggets eller systemets betydning for energiforsyningen.

Beredskapsmyndigheten kan treffe vedtak om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av § 5-2 dersom det anses nødvendig.

Beredskapsmyndigheten kan treffe vedtak om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av tidligere vedtak dersom det anses nødvendig.

§ 5-8. Analyse

Virksomhet som planlegger å bygge eller vesentlig endre eller utvide anlegg som er eller vil være klassifisert etter § 5-2, skal på bakgrunn av anleggets klasse etter § 5-2 eller enkeltvedtak, foreta en risiko- og sårbarhetsanalyse og prosjektere, utføre og sikre anlegg og system som angitt i denne forskrift.

§ 5-9. Meldeplikt om sikringstiltak

Virksomheter som planlegger å bygge, endre eller utvide konsesjonspliktige anlegg, skal senest ved søknad om konsesjon sende beredskapsmyndigheten skriftlig melding om hvilken klasse anlegget vil bli bygget etter, jf § 5-2.

For driftskontrollsystemer og annet uten konsesjonsplikt gjelder en tilsvarende plikt om melding i god tid før byggestart.

Melding skal gis elektronisk eller på annen måte som beredskapsmyndigheten bestemmer. Meldingen skal være vedlagt den informasjon som beredskapsmyndigheten bestemmer.

§ 5-10. Vakthold

Eier eller driver av kraftforsyningsanlegg som er prioritert for vakthold i ekstraordinære situasjoner, skal bidra til planlegging og gjennomføring av vaktholdet i samarbeid med politi og forsvar.

Plikten omfatter blant annet:

- a. Påvise anleggets vitale deler og beskaffenhet forøvrig.
- b. Anskaffe materiell for sikring av anlegget og gjennomføre øvrige tiltak for å hjelpe vaktstyrken.
- c. Tilrettelegge for øvelser på anleggets område.

Beredskapsmyndigheten kan etter denne paragraf gi nærmere bestemmelser for objektsikring og gi bestemmelser for gjennomføring av øvelser i høyspenningsanlegg.

§ 5-11. Besøksrestriksjoner

Alle driftssentraler i klassifiserte driftskontrollsystemer, og alle energianlegg klassifisert i klasse 3, skal ha besøksrestriksjoner. Beredskapsmyndigheten kan vedta at også energianlegg i klasse 2 skal ha besøksrestriksjoner.

Ved anlegg underlagt besøksrestriksjoner skal:

- a. De besøkende følge en fast avgrenset rute.

- b. De besøkende til enhver tid være ledsaget av en erfaren og ansvarlig representant for anlegget.
- c. Det ikke gis opplysninger om sensitiv informasjon etter § 6-2.
- e. Fotografering være forbudt med mindre spesiell tillatelse er innhentet fra ansvarlig representant for anlegget.

Driftssentraler i klasse 3 skal ha besøksforbud. Beredskapsmyndigheten kan vedta besøksforbud for andre energianlegg i klasse 3.

Kapittel 6. Informasjonssikkerhet

§ 6-1. Identifisering av sensitiv informasjon og rettmessige brukere

Alle KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er sensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den.

Identifiseringen av hva som er sensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.

Med rettmessig bruker menes fysiske eller juridiske personer som har tjenstlig behov for sensitiv informasjon. Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for sensitiv informasjon innenfor sin virksomhet og kan avgjøre om det er tjenstlig behov for å videreformidle sensitiv informasjon fra virksomheten til andre utenfor egen virksomhet. Beredskapsmyndigheten kan i tvilstilfeller avgjøre hvem som er rettmessig bruker.

§ 6-2. Sensitiv informasjon

Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.

Med sensitiv informasjon menes spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen, herunder:

- a. Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband.
- b. Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg.
- c. Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.
- d. Oversikt over fordelingsnett til samfunnskritiske funksjoner.
- e. Nøyaktig kartfesting av jordkabler.
- f. Forebyggende sikkerhetstiltak mot bevisst skadeverk.
- g. Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.

- h. Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.
- i. Beredskapsplaner for å håndtere bevisst skadeverk.
- j. Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk.

§ 6-3. Beskyttelse, avskjerming og tilgangskontroll

Alle KBO-enheter skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for sensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.

System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.

Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese sensitiv informasjon.

§ 6-4. Sikkerhetsinstruks

Alle KBO-enheter skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas, og som beskriver identifiseringen som er foretatt i henhold til § 6-1 og hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og skal stille krav til undertegning av taushetserklæring. Sikkerhetsinstruksen skal også omfatte informasjon om at taushetsplikten medfører at sensitiv informasjon ikke skal offentliggjøres.

§ 6-5. Anskaffelser i energiforsyningen

KBO-enheter som setter ut oppdrag til leverandører og andre med oppdrag for eller i energiforsyningen, skal påse at disse er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. Det skal også i avtale opplyses at beredskapsmyndigheten kan føre tilsyn med etterlevelsen av disse bestemmelsene. Tilsvarende opplysningsplikt gjelder for leverandører når disse inngår kontrakt med underleverandører.

Plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves.

Bestemmelsene i første og annet ledd gjelder tilsvarende når KBO-enheter setter ut oppdrag for prosjektering, installering, vedlikehold og feilretting av driftskontrollsystemet.

§ 6-6. Begrenset anbudsinnbydelse

Anbudsinnbydelser og lignende skal begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller sensitiv informasjon om energiforsyningen blir offentlig tilgjengelig gjennom anbudsdokumentene.

Forståelsen av begrenset anbudsinnbydelse bygger på anskaffelsesregelverket.

§ 6-7. Personkontroll

Person som vil kunne få tilgang til informasjon som er sikkerhetsgradert etter lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven), skal være sikkerhetsklarert og autorisert. Autorisasjon for BEGRENSET kan skje uten forutgående sikkerhetsklarering.

§ 6-8. Sikkerhetskopier

Virksomheten skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppretting av energiforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.

Nødvendig dokumentasjon om energisystemet og som lagres på datamedia, skal også foreligge som papirutskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted som er lett tilgjengelig for virksomheten.

Kapittel 7. Beskyttelse av driftskontrollsystem

§ 7-1. Generell plikt til å beskytte driftskontrollsystemet

Alle virksomheter med driftskontrollsystem skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser, herunder mot alle typer uautorisert tilgang for å hindre misbruk og spredning av skadelig programvare og lignende.

Alle virksomheter med driftskontrollsystem er underlagt bestemmelsene om klassifisering og sikringsplikt etter kapittel 5.

§ 7-2. Overordnede sikkerhetsregler

Virksomheten skal fastsette sikkerhetskrav for bruk, utvikling, drift, systemvedlikehold, sikring med mer av driftskontrollsystem slik at overvåking og kontroll av energiforsyningen kan utføres på en sikker måte.

Sikkerhetskravene skal gjennomgås minimum årlig for å klarlegge om de er hensiktsmessige i forhold til virksomhetens behov, om de etterleves, og om kravene gir tilfredsstillende beskyttelse av driftskontrollsystemet.

§ 7-3. Dokumentasjon av driftskontrollsystemet

Virksomheten skal til enhver tid ha oppdatert dokumentasjon av driftskontrollsystemet.

I dokumentasjonen skal det inngå en oversikt over alle sikkerhetstiltak som er implementert. Dokumentasjonen skal også omfatte en oppdatert skjematisk fremstilling av driftskontrollsystemets logiske og fysiske nettverk som viser eventuelle tilgangspunkt mellom driftskontrollsystemet og andre nettverk.

§ 7-4. Kontroll med brukertilgang

Virksomheten skal ha kontrollordninger for tildeling, endring, sletting og vurdering av korrekt tilgang til driftskontrollsystemet.

Virksomheten skal til enhver tid kunne kontrollere hvilken person som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes.

Kontrollordningene skal gjennomgås minimum årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå.

§ 7-5. Kontroll ved endringer i driftskontrollsystemet

Virksomheten skal ha kontrollordninger for vurdering, testing og godkjenning av endringer i driftskontrollsystemet før disse utføres, for å hindre utilsiktede feil og påføring av nye sårbarheter.

§ 7-6. Kontroll med utstyr i driftskontrollsystemet

Utstyr som benyttes i driftskontrollsystemet tillates ikke brukt i andre nettverk eller løsninger utenom driftskontrollsystemet, heller ikke midlertidig.

Utstyr som benyttes for å etablere logiske eller fysiske skiller mellom prosessnettverk i driftskontrollsystemet og andre nettverk, skal ha effektive kontrollordninger som hindrer uautorisert tilgang mellom skillene.

Virksomheten skal ha en oppdatert oversikt over utstyr av vesentlig betydning for driftskontrollsystemets funksjon.

Virksomheten skal ha en effektiv kontrollordning for sikker avhending av utstyr som har blitt benyttet i driftskontrollsystemet.

Det er ikke tillatt å bruke personlig eid utstyr i driftskontrollsystemet.

Bruk av trådløse datanettverk i driftskontrollsystemet er ikke tillatt.

Beredskapsmyndigheten kan i særskilte tilfeller forby bruk av utstyr.

§ 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd

Virksomheten skal etablere kontrollordninger for å sikre effektiv håndtering av feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemets funksjon.

Virksomheten skal ha tilgang til tilstrekkelig personell med nødvendig kompetanse som uten unødig opphold kan håndtere forhold angitt i første ledd.

Alle sikkerhetsbrudd og hendelser skal registreres.

Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf også § 2-6.

§ 7-8. Beredskap ved svikt i driftskontrollsystemet

Virksomheten skal ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet.

§ 7-9. Bemanning av driftssentral

Virksomheten skal til enhver tid ha tilstrekkelig og tilgjengelig autorisert personell med nødvendig kompetanse, slik at driftskontrollfunksjonen kan utøves uten ugrunnet opphold.

Virksomhetens risiko- og sårbarhetsanalyse skal ligge til grunn for valg av bemanningens størrelse samt omfang av ordninger for påkalling av ekstra personell ved behov, jf §§ 2-4 og 5-8.

§ 7-10. Ekstern tilkobling til driftskontrollsystem

Virksomheten skal ha kontrollordninger for å godkjenne, vedlikeholde og avvikle ordninger for ekstern tilkobling til driftskontrollsystemet, samt funksjoner for innstilling av vern. En særskilt vurdering skal ligge til grunn for godkjenning av løsning.

Kun autorisert personell kan gis adgang til driftskontrollsystemet gjennom ekstern tilgang. Virksomheten skal ha kontrollordninger for vurdering, tildeling, endring og tilbaketrekking av autorisasjon. Virksomheten skal ha en oppdatert liste over alle som er autorisert.

Det skal foreligge en egen forhåndsavtalt prosedyre for ekstern tilkobling til driftskontrollsystemet.

Det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.

For fjernvarmeanlegg der hele eller deler av driftskontrollfunksjonen utføres av selskap som ikke er KBO-enhet, må vedkommende KBO-enhet påse at hele driftskontrollsystemet beskyttes etter relevante bestemmelser i denne forskrift.

§ 7-11. Systemredundans i driftskontrollsystemet

Virksomheten skal vurdere behovet for redundans i driftskontrollsystemet basert på lokale forhold og risikoanalyse.

§ 7-12. Sammenkobling mellom avanserte måle- og styringssystem (AMS) og driftskontrollsystem

Dersom virksomheten har integrert funksjonalitet for bryting og begrensnings av effektuttak i avanserte måle- og styringssystem (AMS), jf forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av netjtjenester § 4-2 e, i virksomhetens driftskontrollsystem, skal IKT-system med tilhørende utstyr som benyttes til denne funksjonen, sikres i henhold til driftskontrollsystemets klasse.

Med integrert funksjonalitet menes at funksjonen for å bryte og begrense effekt ved AMS utøves fra virksomhetens driftssentral, og at man benytter samme utstyr og infrastruktur som virksomheten benytter i driftskontrollsystemet.

Bestemmelsen gjelder til og med det utstyr eller punkt der signalene for å bryte og begrense effektuttak adskilles fra signalene i driftskontrollsystemet.

§ 7-13. Beskyttelse mot elektromagnetisk puls og interferens

Virksomheten skal vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls (EMP) eller elektromagnetisk interferens (EMI). Dersom sårbarheter avdekkes, skal det gjennomføres sikrings- eller beredskapstiltak etter driftskontrollsystemets betydning for sikker drift og gjenoppretting av funksjon i energiforsyningen.

§ 7-14. Særskilte krav til driftskontrollsystem klasse 2

Foruten de generelle krav til beskyttelse av driftskontrollsystemet, skal virksomheter med driftskontrollsystem i klasse 2 oppfylle følgende tilleggskrav:

a. Sikkerhetskopier

Virksomheten skal jevnlig teste at gjenoppretting av elektroniske sikkerhetskopier fungerer etter hensikten.

b. Sikkerhetsrevisjon

Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene faktisk er etablert og fungerer etter sin hensikt.

c. Overvåking og logging

Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.

d. Utilgjengelig driftssentral

Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid.

e. Bemanning av driftssentral

Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold.

Virksomheten skal senest innen én time kunne bemanne driftssentralen.

Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.

f. Ekstern tilkobling til driftskontrollsystemet

Ved tilkobling fra leverandører skal driftssentralen være bemannet.

Virksomheten skal ha kontrollordning for korrekt autentisering av de personene som er autorisert til å benytte ekstern tilkobling for adgang til driftskontrollsystemet.

Virksomheten må sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheten skal utarbeide interne regler for hva som er et sikkert sted.

Den eksterne tilkoblingen skal kun åpnes når det er behov for å få tilgang til driftskontrollsystemet. Tilkoblingen skal være lukket når den ikke er i bruk.

Det skal foreligge en egen skriftlig prosedyre for ekstern tilkobling.

Dersom KBO-enheten kan foreta styring av anlegg i energiforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person.

Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

g. Systemredundans

Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett.

Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans.

Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner.

Det skal etableres reparasjonsberedskap for alt samband, jf kapittel 4 og § 7-8.

h. Særskilt om dublering

Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil ikke rammer alle dublerede system samtidig, jf § 7-7.

i. Beskyttelse mot EMP og EMI

Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer.

j. Sikker tidsreferanse

Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse.

§ 7-15. Særskilte krav til driftskontrollsystem klasse 3

Foruten de generelle kravene samt særskilte krav til beskyttelse av driftskontrollsystem i klasse 2, skal virksomheter med driftskontrollsystem i klasse 3 oppfylle følgende tilleggskrav:

a. Reserve driftssentral

Virksomheten skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge.

Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner.

Reserve driftssentral skal utføres med sikringsnivå i henhold til vedtatt klasse for driftskontrollsystemet for øvrig, jf § 5-6.

b. Bemanning av driftssentral

Driftssentralen skal være døgnbemannet.

Opptrapping av bemanningen skal kunne skje innen én time etter at påkalling er gjort.

Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf § 7-9, andre ledd.

c. Ekstern tilkobling til driftskontrollsystemet

Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.

d. Systemredundans

Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem.

Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf kapittel 5.

e. Beskyttelse mot EMP og EMI

Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak.

I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.

f. Fastsettelse av særlige krav til bemanning

For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf § 5-7.

§ 7-16. Vern av kraftsystem i regional- og sentralnett

Kommunikasjonsbaserte vernsystemer i sentral- og regionalnett skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftforsyningssystemet.

§ 7-17. Mobile radionett - driftsradio

Alle enheter i KBO som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon, skal ha tilgang til et mobilt sambandssystem. Dette sambandssystemet skal:

- a. Omfattes av den generelle sikringsplikten etter § 5-1.
- b. Til enhver tid holdes i funksjonsdyktig stand, være klar til bruk, og det skal være rask tilgang på kritiske reservedeler og kompetanse på feilretting.
- c. Kunne betjenes av personell med nødvendig kompetanse til bruk.
- d. Ha tilstrekkelig dekningsgrad for kraftforsyningens anlegg og drift.
- e. Kunne fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett.
- f. Ha tilstrekkelig nødstrøm ved omfattende eller langvarige strømbrudd, herunder et nødstrømssystem med automatisk start og minimum 48 timer selvstendig driftstid.
- g. Ha nødvendig funksjonalitet med blant annet direkte apparat til apparat-kommunikasjon, gruppesending og felles oppkall.
- h. Kunne fungere som reservesamband om annet viktig samband svikter.
- i. Der hvor radionettet benytter anlegg tilhørende et klassifisert driftskontrollsystem eller hvor det må regnes som en del av dette, skal sambandssystemet beskyttes i henhold til driftskontrollsystemets klasse.
- j. Der hvor radionettet er digitalisert og f.eks. baserer seg på IP-løsninger, skal dette sikres mot uautorisert tilgang, spredning av uønsket programvare, urettmessig overtakelse m.m. etter relevante bestemmelser i denne forskrift.

Kapittel 8. Avsluttende bestemmelser

§ 8-1. Kontroll

Beredskapsmyndigheten fører kontroll med at bestemmelser gitt i eller i medhold av denne forskriften overholdes.

Virksomheten skal medvirke til gjennomføring av kontroll. Dette omfatter blant annet å fremskaffe dokumentasjon og opplysninger som er nødvendige for å gjennomføre kontroll, og gi beredskapsmyndigheten adgang etter energiloven § 9-5 annet ledd.

§ 8-2. Pålegg

Beredskapsmyndigheten kan gi de pålegg som er nødvendige for gjennomføring av bestemmelser gitt i eller i medhold av denne forskrift.

§ 8-3. Dispensasjon

Beredskapsmyndigheten kan i særlige tilfeller gi dispensasjon fra bestemmelser gitt i eller i medhold av denne forskrift.

§ 8-4. Tvangsmulkt

Ved overtredelse av bestemmelser gitt i eller i medhold av denne forskrift, kan beredskapsmyndigheten ilegge tvangsmulkt i medhold av energiloven § 10-3.

§ 8-5. Overtredelsesgebyr

Ved overtredelse av bestemmelsene i kapittel 2 til 7, inkludert vedleggene til kapittel 5, og vedtak truffet i medhold av § 8-3 kan det ilegges overtredelsesgebyr i medhold av energiloven §§ 10-7 og 10-8.

§ 8-6. Straff

Overtredelse av bestemmelsene i kapittel 2-8, inkludert vedleggene til kapittel 5, kan straffes med bøter eller fengsel i medhold av energiloven § 10-5.

§ 8-7. Gebyr til beredskapsmyndigheten

Til dekning av beredskapsmyndighetens utgifter til arbeidet med energiforsyningsberedskap innkreves et årlig gebyr.

Gebyret fastsettes for det enkelte kraftselskap på grunnlag av installert ytelse i kraftverk, transformatorstasjoner og nettstasjoner pr. 1. januar det år gebyret beregnes for. Satsene skal reguleres slik at de samlede gebyrer tilsvarer de faktiske utgifter beredskapsmyndigheten har med beredskapsarbeidet.

§ 8-8. Ikrafttreden

Denne forskriften trer i kraft 1. januar 2013. Fra samme tid oppheves forskrift 16. desember 2002 nr. 1606 om beredskap i kraftforsyningen.

§ 8-9. Forholdet til eldre vedtak om klassifisering og overgangsregler

Vedtak om sikring eller andre vedtak i medhold av forskrift 16. desember 2002 nr. 1606 om beredskap i kraftforsyningen truffet etter 1. januar 2003 og før 1. januar 2013 står fortsatt ved lag inntil de blir endret eller opphevet i medhold av denne forskrift.

Anlegg som er idriftssatt før 1. januar 2013, og som ikke er omfattet av vedtak omtalt i første ledd, klassifiseres etter denne forskrift, men slik at sikringstiltak etter kapittel 5 kan tilpasses bygningsteknisk utforming og tidligere pålegg om fysisk sikring. Ved vesentlig ombygging eller utvidelse vil kravene etter kapittel 5 gjelde fullt ut for den del av anlegget som endres.

Vedtak om beredskapsmessige forhold til kraftforsyningen om annet enn klassifisering og sikringstiltak truffet før 1. januar 2003, og som ikke er erstattet av senere vedtak eller forskrifter står ved lag så langt de passer inntil de blir endret eller opphevet i medhold av denne forskrift.

Alle anlegg som er idriftssatt etter 1. januar 2013 skal klassifiseres og sikres etter denne forskrift. Dette gjelder selv om de har fått konsesjon før 2013. For disse anleggene gjelder en overgangsperiode på 2 år. Beredskapsmyndigheten kan gi én dispensasjon fra dette. Slik dispensasjon kan kun gis én gang for hvert anlegg for en periode på inntil 2 år.

Vedlegg 1 til § 5-4: Særlige krav til sikring for anlegg klassifisert i klasse 1

Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 1.1 til 1.3.

1.1 For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg gjelder følgende krav:

- 1.1.1 Det skal etableres en adgangskontrollert sone som omfatter alle adkomster til anlegget. Fysisk sikring skal som et minimum omfatte et solid bygg med dører/porter, vinduer og øvrige adkomster. Disse skal oppfylle krav til normalt sikringsnivå etter fastsatte normer.
- 1.1.2 Brannsikring skal oppfylle krav i henhold til andre relevante forskrifter og normal brannmotstand etter fastsatt norm.
- 1.1.3 Rom for lokal driftskontroll, styring og samband skal være egne adgangskontrollerte soner, og skal oppfylle krav til normalt sikringsnivå og brannmotstand etter fastsatte normer.
- 1.1.4 For egen stasjonsstrømforsyning skal anlegget ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Et mobilt aggregat må kunne kobles til innenfor batteritiden. Anlegget må samlet sett ha en gangtid på minst ett døgn.
- 1.1.5 Det skal være tilgang på reserver for viktige komponenter.

1.2 For driftskontrollsystemer gjelder følgende krav:

1.2.1 Driftssentraler

- 1.2.1.1 Driftssentraler skal plasseres i et bygg med normal brann- og innbruddssikkerhet.
- 1.2.1.2 Skal ha et effektivt innbrudds- og brannvarslingssystem.
- 1.2.1.3 Skal være normalt fysisk sikret etter fastsatt norm.
- 1.2.1.4 Skal være utstyrt med avbruddsfri strømforsyning og mulighet for tilkobling av mobilt nødstrømsaggregat, med en samlet gangtid på minst ett døgn.
- 1.2.1.5 Skal ha et alternativt opplegg for utøvelse av viktige funksjoner for drift og ledelse i en ekstraordinær situasjon.

1.2.2 For sambandsanlegg gjelder følgende krav:

- 1.2.2.1 Sambandsanlegg regnes normalt som en del av det driftskontrollsystem de betjener og skal planlegges og utføres etter de påregnelige påkjenninger de kan bli utsatt for.

- 1.2.2.2 Anlegget skal sikres mot uønskede hendelser og handlinger som innbrudd, hærverk, sabotasje og brann.
- 1.2.2.3 Anlegget skal utstyres med nødstrøm med automatisk start og gangtid på minst ett døgn.
- 1.2.2.4 Anlegget skal også oppfylle kravene som fremgår av § 4-7.

1.3 For kraftledninger gjelder følgende krav:

- 1.3.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessige betydning.

Vedlegg 2 til § 5-5: Særlige krav til sikring for anlegg klassifisert i klasse 2

Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5.

2.1. For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:

- 2.1.1 Anleggets sikringsnivå skal ivaretas gjennom en kombinasjon av blant annet følgende tiltak:
 - a. Uønskede hendelser og handlinger skal oppdages raskt og håndteres av et effektivt reaksjonsmønster.
 - b. Fysisk og elektrisk utførelse og beskyttelse skal være på et nivå som begrenser tap av funksjon og ødeleggelse.
 - c. Gjenoppretting av eventuelle funksjonstap skal skje uten ugrunnet opphold.
 - d. Redundans i anlegget eller kraftsystemet.
- 2.1.2 Tiltakene skal komplettere hverandre og gi en balansert helhet.
- 2.1.3 Anlegget skal fungere uavhengig av de strømutfall som kan forekomme i ordinær strømforsyning og påregnelige feil i eget strømforsyningssystem.
- 2.1.4 Anlegget skal kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriften, jf § 4-2.

2.2. For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:

- 2.2.1 Anlegget skal være utstyrt med effektive og pålitelige alarmer for brann, innbrudd, elektriske feil og feil i styresystemer, samt ha etablert tiltak for effektiv reaksjon.
- 2.2.2 Viktige anleggsdeler som driftsbygg, innendørs apparatanlegg, muffeanlegg og anlegg for stasjonsstrøm og styring skal ha god skallsikring etter fastsatte normer.
- 2.2.2 Driftskontrollrom og andre rom for styring og samband skal være egne adgangskontrollerte soner med middels sikringsnivå og brannmotstand etter fastsatte normer.
- 2.2.4 Alle hovedtransformatorer med tilhørende adkomster skal sikres fra alle kanter med bygg eller lignende, med god beskyttelse etter fastsatte normer for sikring og brannmotstand.
- 2.2.5 Anlegget skal ha dublerede føringer for stasjonsstrøm og styresignaler.

- 2.2.6 Skal som hovedregel ha dublering av de viktigste komponenter for anleggets primære funksjoner. Dette gjelder bl.a. samleskinner, skillebrytere, samt annen nødvendig utrustning.
- 2.2.7 Skal ha et dublert nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Om det ikke er installert et stasjonært nødstrømsaggregat, må et mobilt aggregat kunne kobles til innenfor batteritiden under maksimal belastning. Anlegget må samlet sett ha en gangtid på minst to døgn.
- 2.2.8 Viktige kabler for driftskontroll og styre- og nødstrøm skal så langt som mulig, fysisk separeres fra høyspentkabler.

2.3 For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:

- 2.3.1 Kraftstasjoner i fjell skal ha en adgangskontrollert og fysisk sikret sone omfattende alle adkomster. Denne sonen skal oppfylle krav til godt sikringsnivå etter fastsatte normer for sikring. Herunder skal alle stasjoner ha minst én solid og låsbar stålport eller lignende i alle adkomster.
- 2.3.2 Kraftstasjoner i dagen skal ha god fysisk sikring med minimum et solid bygg med dører/ porter, vinduer og øvrige adkomster etter fastsatte normer for sikringsnivå.
- 2.3.3 For kraftstasjoner i fjell og i dagen skal vitale komponenter som må plasseres utendørs, sikres etter samme krav som for transformatorstasjon, koblingsanlegg mv. i klasse 2.
- 2.3.4 Anleggets adkomster og vitale områder skal være utstyrt med effektive og pålitelige alarmer for brann, innbrudd, elektriske feil, og feil i styresystemer, samt ha etablert effektiv reaksjon for slike uønskede hendelser og handlinger.
- 2.3.5 Anlegget skal brannsikres og seksjoneres på hensiktsmessig måte med god brannmotstand etter fastsatt norm.
- 2.3.6 Driftskontrollrom, rom for styring og samband og lignende skal være egne og godt beskyttede adgangskontrollerte soner etter fastsatte normer for sikring og brannmotstand.
- 2.3.7 Anlegget skal som hovedregel ha dublering av de viktigste komponenter og annen nødvendig kontrollutrustning, samt ha dublerte føringer for stasjonsstrøm og styresignaler. Det kreves ikke redundans for anleggets hovedkomponenter, som turbin, generator mv.
- 2.3.8 Skal ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Om det ikke er installert et stasjonært nødstrømsaggregat, må et mobilt aggregat kunne kobles til innenfor batteritiden under maksimal belastning. Anlegget må samlet sett ha en gangtid på minst to døgn.
- 2.3.9 Viktige kabler for driftskontroll og styre- og nødstrøm skal så langt som mulig fysisk separeres fra høyspentkabler.
- 2.3.10 Minst ett aggregat skal normalt kunne starte på spenningsløst nett (svart nett),

2.4 For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 2.1:

2.4.1 Driftssentraler

- 2.4.1.1 Driftssentraler skal plasseres i et bygg med god brann- og innbruddssikkerhet.
- 2.4.1.1 Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, varsling og rask reaksjon ved uønskede hendelser og handlinger.
- 2.4.1.2 Skal være en egen fysisk sikret adgangskontrollert sone og utføres som egen branncelle med god brannsikkerhet og brannmotstand etter fastsatt norm.
- 2.4.1.3 Viktige komponenter og systemer skal ha redundans slik at én enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 2.4.1.4 Operatørrom og andre bygningsdeler av vesentlig betydning for driftskontrollfunksjonene skal være normalt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.
- 2.4.1.5 Driftssentralens data-, sambands- og øvrige systemer som er nødvendige for driften av kraftsystemet, skal forsynes fra to uavhengige strømkurser. Dette inkluderer et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning som skal en driftstid på minst seks timer. Dersom det ikke er installert permanent nødstrømsaggregat, skal et mobilt nødstrømsaggregat kunne kobles til og være tilgjengelig godt innenfor batterikapasiteten. Nødstrømsanlegget skal samlet sett ha automatisk start og gangtid på minst to døgn.
- 2.4.1.6 Skal ha et alternativt opplegg for utøvelse av alle viktige funksjoner i en ekstraordinær situasjon.

2.4.2 Sambandsanlegg gjelder:

- 2.4.2.1 Sambandsanlegg regnes normalt som en del av det driftskontrollsystem de inngår i.
- 2.4.2.2 Anlegget skal planlegges og utføres slik at de tåler de maksimale påkjenninger de kan bli utsatt for.
- 2.4.2.3 Anlegget skal sikres mot uønskede hendelser og handlinger som innbrudd, hærverk, sabotasje og brann.
- 2.4.2.4 Anlegg med god tilgjengelighet skal utstyres med nødstrøm med automatisk start og gangtid på minst to døgn. For vanskelig tilgjengelige anlegg skal inntil 14 døgn vurderes.
- 2.4.2.5 Anlegget skal også oppfylle kravene som fremgår av kapittel 7.

2.5 For kraftledninger gjelder følgende krav:

- 2.5.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessig betydning.
- 2.5.2 For kabler skal i tillegg viktige komponenter som endemuffer og skjøter beskyttes. Alternativt kan det anskaffes reservekomponenter som lagres på sikkert sted, og det skal være tilgang til reservekabel med mer etter § 4-4.
- 2.5.3 Gjenoppretting av funksjonstap skal skje uten ugrunnet opphold.

2.6 For fjernvarmeanlegg gjelder følgende krav i tillegg til kravene i punkt 2.1:

- 2.6.1 Beredskapsmyndigheten kan fastsette særlige krav til sikring av fjernvarmeanlegg.

Vedlegg 3 til § 5-6: Særlige krav til sikring for anlegg klassifisert i klasse 3

Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 3.2 til 3.6.

3.1 For transformatorstasjoner, koblingsanlegg/-stasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav:

- 3.1.1 Anleggets sikringsnivå skal ivaretas gjennom en kombinasjon av blant annet følgende tiltak:
 - a. Alle uønskede hendelser og handlinger skal oppdages straks, kunne verifiseres og håndteres av et effektivt reaksjonsmønster.
 - b. Fysisk og elektrisk utførelse og beskyttelse skal være på et nivå som forebygger eller forhindrer tap av funksjon og ødeleggelse.
 - c. Gjenoppretting av eventuelle funksjonstap skal skje så raskt som fysisk mulig.
 - d. Redundans i anlegget eller kraftsystemet.
- 3.1.2 Tiltakene skal komplettere hverandre og gi en balansert helhet.
- 3.1.3 Anlegget skal fungere uavhengig av ordinær strømforsyning og feil i anleggets eget strømforsyningssystem. Funksjon skal opprettholdes også ved upåregnelige og langvarige strømutfall.
- 3.1.4 Alle anlegg skal samtidig og så raskt som mulig kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriften, jf § 4-2.

3.2. For transformatorstasjoner og koblingsanlegg/-stasjoner gjelder følgende krav i tillegg til kravene i over nevnte punkt 3.1:

- 3.2.1 Anlegget skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmering, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger.
- 3.2.2 Anlegget skal ha en fysisk områdesikring som effektivt hindrer inntrengning.
- 3.2.3 Anlegget skal ha god avstand til ikke-avspærrede områder.
- 3.2.4 Viktige anleggsdeler som driftsbygg, innendørs apparatanlegg, mufteanlegg og anlegg for stasjonsstrøm og styring, samt store og viktige komponenter med lang leveringstid, skal ha god skallsikring etter fastsatte normer for sikringsnivå.
- 3.2.5 Driftskontrollrom, datarom og andre rom for styring og samband skal være egne adgangskontrollerte soner, godt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.

- 3.2.6 Alle hovedtransformatorer skal skallsikres fra alle kanter til over topp endemuffer ved hjelp av fjell eller transformatorceller av solid dobbeltarmert betong eller tilsvarende, og være konstruert og oppført etter anerkjente byggenormer. De skal herunder beskyttes og seksjoneres med høy brannmotstand etter fastsatt norm. De skal ha låsbare dører/porter eller fast montert gitter med høyt sikringsnivå etter fastsatt norm i alle mulige adkomster og lufteåpninger opptil minimum tre meter fra bakkeplan eller liknende.
- 3.2.7 Anlegget skal ha dublerter og fysiske uavhengige kabelføringer for hhv. styring og samband, nød- og stasjonsstrøm og høyspent, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 3.2.8 Anlegget skal som hovedregel ha dublering av de viktigste komponenter for anleggets primære funksjoner. Dette gjelder bl.a. samleskinner, effekt- og skillebrytere, samt annen nødvendig utrustning. Hovedtransformatorers funksjon skal ha redundans i anlegg eller system.
- 3.2.9 Anlegget skal ha et elektrisk og fysisk dublert system for egen stasjonsstrøm med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften av stasjonen forsynes fra to helt uavhengige og separerte strømkurser-/ systemer. Dette skal også omfatte et nødstrømsystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning og minimum har en samlet driftstid på minst seks timer. Det skal være installert et stasjonært nødstrømsaggregat med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrytning og minst tre døgn selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Nødstrømsystemet skal tåle de maksimalbelastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling av nødvendig utstyr og liknende.
- 3.2.10 Dublering etter punkt 3.2.7 til 3.2.9 skal så langt som mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.
- 3.2.11 Det skal gjøres en vurdering av konsekvensene av geomagnetisk induserte strømmer, og iverksettes relevante tiltak for å beskytte hovedtransformatorer.

3.3 For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:

- 3.3.1 Alle vitale komponenter skal legges i beskyttende fjellrom og det skal etableres en omsluttende adgangskontrollert og fysisk sikret sone som omfatter alle mulige adkomster med høyt sikringsnivå etter fastsatt norm. Herunder skal alle stasjoner ha minst én solid og låsbar stålport eller lignende i alle adkomster. Vitale komponenter som må legges i dagen, sikres som for transformatorstasjon, koblingsanlegg mv. i klasse 3.
- 3.3.2 Anlegget skal seksjoneres på en hensiktsmessig måte med brannsikring som gir høy brannmotstand etter fastsatte normer og relevante forskrifter.

- 3.3.3 Skal ha utstyr og prosedyrer for effektiv deteksjon, alarmer, verifikasjon og reaksjon mht. uønskede hendelser og handlinger. Som et minimum skal dette omfatte adkomster og stasjonens vitale områder.
- 3.3.4 Driftskontrollrom, rom for styring og samband og lignende skal være egne adgangskontrollerte godt beskyttede soner etter fastsatte normer for hhv. fysisk sikring og brannmotstand.
- 3.3.5 Anlegget skal ha dublerter og fysiske uavhengige kabelføringer for hhv. styring og samband, nød- og stasjonsstrøm og høyspent, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 3.3.6 Skal ha et elektrisk og fysisk dublert system for egen stasjonsstrøm med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften av stasjonen, forsynes fra to uavhengige og separerte strømkurser-/ systemer. Dette skal også omfatte et nødstrømssystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning, og minimum har en samlet driftstid på minst seks timer. Stasjonen skal være utstyrt med en stasjonær selvdrevet anordning for stasjonsstrøm (nødstrømsaggregat, hjelpegenerator eller lignende) med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrytning og minst tre døgn selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom den stasjonære anordning skulle svikte. Nødstrømssystemet skal tåle de maksimalbelastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling og lignende.
- 3.3.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.
- 3.3.8 Det kreves ikke redundans for anleggets hovedkomponenter, som turbin, generator mv.
- 3.3.9 Minst ett aggregat skal normalt kunne starte på spenningsløst nett (svart nett) og kunne drives separat (øydift).

3.4 For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 3.1:

3.4.1 Driftssentraler

- 3.4.1.1 Driftssentraler skal plasseres i et solid bygg med god brann- og innbruddssikkerhet.
- 3.4.1.2 Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger.
- 3.4.1.3 Skal være egen fysisk sikret adgangskontrollerte sone(r) og utføres som egen branncelle(r) med høy brannsikkerhet og brannmotstand etter fastsatte normer.

- 3.4.1.4 Operatørrom og andre bygningsdeler av vesentlig betydning for driftskontrollfunksjonene skal være godt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.
- 3.4.1.5 Alle komponenter og systemer skal utføres fullredundant med bl.a. dublerter og fysiske uavhengig prosessutstyr, føringsveier for strøm, signaler og sambandsutrustning, samt annen nødvendig utrustning, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
- 3.4.1.6 Skal ha et elektrisk og fysisk dublert system for egen strømforsyning med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften forsynes fra to uavhengige og separerte strømkurser-/systemer. Dette skal også omfatte et nødstrømsystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning, og minimum har en samlet driftstid på minst seks timer. Det skal være installert et stasjonært nødstrømsaggregat med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrudd og minst tre døgns selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Nødstrømsystemet skal tåle de maksimale belastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling av nødvendig utrustning, og lignende.
- 3.4.1.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres
- 3.4.1.8 Skal ha et beredskapsrom og/ eller fysisk alternativ sted med opplegg for utøvelse av alle viktige funksjoner i en ekstraordinær situasjon.

3.4.2 Sambandsanlegg gjelder:

- 3.4.2.1 Anlegget skal utføres så fysisk, elektrisk og elektronisk robust at det tåler påregnelig uvær og andre ytre påkjenninger, herunder atmosfæriske og elektromagnetiske forstyrrelser
- 3.4.2.2 Utsatte anleggsdeler som kabler, master og antenner/ radiospeil skal utføres særlig robuste, og bygg med adkomster som dører og vinduer må gis god sikring etter fastsatte normer for fysisk sikring.
- 3.4.2.3 Anlegg med god tilgjengelighet året rundt skal utstyres med nødstrøm med automatisk start og gangtid på minst tre døgn, men for vanskelig tilgjengelige anlegg må dette etter forholdene økes til 30 døgn.
- 3.4.2.4 Anlegget skal også oppfylle kravene som fremgår av kapittel 7.

3.5 For kraftledninger gjelder følgende krav:

- 3.5.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessige betydning.
- 3.5.2 For kabler skal i tillegg viktige komponenter som endemuffer og skjøter beskyttes. Alternativt kan det anskaffes reservekomponenter som lagres på sikkert sted, og det skal anordnes reservekabel med nødvendig utstyr etter § 4-4.
- 3.5.3 Gjenoppretting av eventuelle funksjonstap skal skje så raskt som fysisk mulig.

Vedlegg 4: Henvisning til normer og standarder i forskriften.

Alle KBO-enheter skal dokumentere hvilke normer som er brukt når dette er relevant for å oppfylle denne forskrift. De normer det henvises til er gjeldende *Norsk standard* (NS) basert på likeverdig europeisk norm (EN):

NS-EN 13501	Brannklassifisering av byggevarer og bygningsdeler
NS-EN 1627	Inngangsdører, vinduer, påhengsvegger, gitter og skodder - Innbruddssikkerhet - Krav og klassifisering
NS-EN 1303	Bygningsbeslag - Låssylindere - Krav og prøvingsmetoder
NS-EN 12209	Bygningsbeslag - Låser og fallelåser - Mekanisk betjente låser, fallelåser og beskyttelseskåper - Krav og prøvingsmetoder
NS-EN 12320	Bygningsbeslag - Hengelåser og hengelåsbeslag - Krav og prøvingsmetoder
NS-EN 356	Bygningsglass - Sikkerhetsruter - Prøving og klassifisering av motstand mot innbrudd og hærverk
NS-EN 1990	Eurokode - Grunnlag for prosjektering av konstruksjoner
NS-EN 1992	Eurokode 2: Prosjektering av betongkonstruksjoner - Del 1-1: Allmenne regler og regler for bygninger

Andre normer kan for eksempel være utarbeidet av *Forsikringsselskapenes Godkjennelsesnevnd* (FG).

I tilfeller hvor normer ikke kan følges, eksempelvis fordi det ikke finnes relevante godkjente produkter eller på grunn av andre hensyn, skal det dokumenteres at valgt løsning oppfyller forskriftens krav gjennom et likeverdig sikringsnivå.

Vedlegg 1-14

Vedlegg 1

Melding om sikring av konsesjonspliktige anlegg

Melding om sikringstiltak for konsesjonspliktig anlegg etter beredskapsforskriften § 5-9, 1. ledd – jf. § 5-2 Klasser

Fyll inn i de grå feltene og skriv ut skjemaet for underskrift. Meldingen vedlegges konsesjonssøknaden.

Anleggets navn og type (jf. bfe § 5-2)

I kommune i fylke

Anleggets eier: [grå felt]	Organisasjonsnummer:
Anlegget drives av (dersom annen enn eier):	Organisasjonsnummer:
Kryss av for det som planlegges: Nybygg Ombygging/ endring Utvidelse (spesifiser): Eventuell kommentar:	
Fyll ut for den (de) aktuelle type anlegg	
Kraftstasjon Samlet generatorytelse (MVA) etter ferdigstillelse: MVA Eventuell kommentar:	
Transformatorstasjon og / eller omformerstasjon Samlet ytelse (MVA) for hvert omsetningsforhold når ferdig: MVA / kV/kV Eventuell kommentar: MVA / kV/kV Eventuell kommentar: Total ytelse: MVA	
Koblingsstasjon kV Antall avganger Eventuell kommentar:	
Ledning /kabel Spenning: Lengde: Type (land, sjø, AC, DC): Eventuell kommentar:	
Fjernvarmeanlegg Samlet installert effekt: Eventuell kommentar:	
Tidsplaner: Anlegget antas påbegynt dato: , Anlegget antas satt i drift dato: Eventuell kommentar:	
Andre opplysninger:	
Kontaktperson for anlegget: Navn: Tittel: Telefon: E-postadresse: ,	
Erklæring Etter vår vurdering skal anlegget plasseres i klasse etter beredskapsforskriftens § 5-2. I så fall erklærer (selskapets navn) herved at vi vil bygge, sikre og drifte anlegget etter beredskapsforskriftens krav til denne klasse.	

.....
Sted

.....
Dato

.....
Firmanavn og stempel

.....
Adresse

.....
Ansvarlig underskrift

Vedlegg 2

Melding om klassifisering av driftskontrollsystem

Fyll inn i de grå feltene og skriv ut skjemaet for underskrift

Meldingen gjelder:

(sett kryss)

Nyinstallasjon Utvidelse Annen endring som kan påvirke anleggets klasse

Navn på virksomhet som eier driftskontrollsystemet:	Organisasjonsnummer
i kommune i fylke	
Anlegget drives av (dersom annen enn eier):	Organisasjonsnummer
Har NVE vedtatt klasse for dette driftskontrollsystemet tidligere? (sett kryss) Ja Nei Hvis ja, angi klasse: og dato for vedtak:	
Gi en kort redegjørelse for hva som skal utføres, og som er grunnen til denne meldingen: Antatt tidspunkt for at de planlagte endringene skal settes i drift:	
Har planene vært diskutert med NVE før denne meldingen ble oversendt? (sett kryss) Ja Nei Hvis ja – hvilken seksjon?	

Opplysninger om driftskontrollsystemets omfang
Kryss av for hva slags type anlegg driftskontrollsystemet overvåker og styrer: Nettanlegg Vannkraftproduksjon Både nett- og vannkraftanlegg Fjernvarmeanlegg Annet (spesifiser)
Driftskontrollsystemet inngår i hvilke nettnivåer / tilknytning til nettet (kryss av det som passer): Sentralnett Regionalnett Distribusjonsnett Fjernvarmenett
Antall anlegg driftskontrollsystemet overvåker og styrer: Transformatorstasjoner inkludert koblingsanlegg i klasse 2: Transformatorstasjoner inkludert koblingsanlegg i klasse 3: Selvstendige koblingsanlegg i klasse 2: Selvstendige koblingsanlegg i klasse 3: Kraftstasjoner i klasse 2: Kraftstasjoner i klasse 3: Antall fjernvarmeanlegg: Annet (spesifiser)

For nettanlegg

Antall forbrukere/kunder som omfattes av anleggene driftskontrollsystemet overvåker og styrer:

Transformatorstasjoner

Samlet nåværende ytelse for stasjonene i klasse 2: MVA / kV.

- Etter eventuell ny installasjon/ombygging: MVA / kV

Samlet nåværende ytelse for stasjonene i klasse 3: MVA / kV

- Etter eventuell ny installasjon/ombygging: MVA / kV

Samlet ytelse for alle stasjonene: MVA (etter eventuelle nyinstallasjoner/ombygginger)

Selvstendige koblingsanlegg

Samlet ytelse for anlegg i klasse 2: kV

Samlet ytelse for anlegg i klasse 3: kV

Total ytelse for alle anleggene: kV

9. Antall avganger til underliggende nett:

For kraftstasjoner:

Samlet nåværende generatorytelse for stasjonene i klasse 2: MW / kV/kV.

- Etter eventuell ny installasjon/ombygging: MW / kV/kV

Samlet nåværende generatorytelse for stasjonene i klasse 3: MW / kV/kV

- Etter eventuell ny installasjon/ombygging: MW / kV/kV

Samlet ytelse for alle stasjonene: MW (etter eventuelle nyinstallasjoner/ombygginger)

Eventuelt antall forbrukere/kunder som omfattes av anleggene driftskontrollsystemet overvåker og styrer:

Er det tilrettelagt for øydrift i noen av områdene der kraftstasjonene er lokalisert eller kan forsyne?

(sett kryss)

Ja Nei

Hvis ja, kan dette iverksettes gjennom driftskontrollsystemet?

Ja Nei

Utdyp besvarelsen om nødvendig:

For fjernvarmeanlegg

Samlet installert effekt: MW

Antall varmesentraler som overvåkes og styres:

Antall forbrukere/kunder som omfattes av anleggene driftskontrollsystemet overvåker og styrer:

Generelle opplysninger om anleggenes forsyningsmessige viktighet – og som overvåkes og styres av driftskontrollsystemet

Hva slags type objekter finnes i forsyningsområdet/forsynes av produksjonsanleggene

(sett kryss der det passer):

Forsvarsanlegg Kraftkrevende industri Annen industri Sykehus/andre helseinst. Offentlig adm.

Om nødvendig utdyp:

Dokumentasjon som skal medfølge denne meldingen

Tegning eller skisse som viser driftskontrollsystemets logiske oppbygning, samt eventuelle tilkoblinger mot Internett.

Andre opplysninger

Andre opplysninger som er relevant for denne meldingen:

Kontaktperson vedrørende denne meldingen

Kontaktperson om anlegget:

Navn: Tittel: Telefon:

E-postadresse:

Postadresse:

Det skal inngås en sikkerhetsavtale med de firmaer som står for levering og/eller drift av tjenester, samt installasjon av styrings- og kontrollsystemer, samt data- og sambandsutstyr i anlegget/systemet

.....
Sted

.....
Dato

.....
Firmastempel

.....
Adresse

.....
Underskrift

Vedlegg 3

TAUSHETSERKLÆRING

Norges vassdrags – og energidirektorat (NVE) (Navn på KBO-enhet)

Jeg forstår at jeg i forbindelse med mitt arbeid kan få kjennskap til sensitive opplysninger, opplysninger om tekniske innretninger eller drifts-/forretningsforhold av konkurransemessig betydning, forhold av betydning for rikets sikkerhet eller opplysninger som det av andre grunner må sikres konfidensialitet for.

Jeg forplikter jeg meg til å bevare fullstendig taushet overfor uvedkommende om opplysninger som er av en slik art at de er taushetsbelagte eller graderte. Det samme gjelder opplysninger som etter sin art kan unntas fra offentlighet etter offentleglova når det ikke vil være naturlig å praktisere meroffentlighet. Jeg forplikter meg til ikke å bruke slike opplysninger til å skaffe meg selv eller andre en uberettiget vinning.

Jeg er kjent med at jeg herunder skal utvise stor aktsomhet med alle dokumenter, slik at de ikke kommer uvedkommende i hende. Jeg forplikter meg til å rette meg etter gjeldende bestemmelser for behandling og oppbevaring av taushetsbelagte eller graderte dokumenter.

Jeg bekrefter at jeg har satt meg inn bestemmelsene i følgende vedlagte lover og forskrifter:

- Sikkerhetsloven (LOV 1998-03-20-10: Lov om forebyggende sikkerhetstjeneste) §§ 11 og 12
- Energiloven (LOV 1990-06-29-50: Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.) § 9-3
- Beredskapsforskriften (FOR-2012-12-07-1157: Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen) §§ 6-2 og 6-3
- Damsikkerhetsforskriften (FOR 2009-12-18-16: Forskrift om sikkerhet ved vassdragsanlegg) § 7-8
- Offentleglova (LOV 2006-05-19-16: Lov om rett til innsyn i dokument i offentlig verksemd) § 13 (når relevant)
- Forvaltningsloven (LOV 1967-02-10: Lov om behandlingsmåten i forvaltningssaker) §§ 13, 13a-f (når relevant)

Jeg bekrefter at jeg er kjent med at:

- brudd på taushetsplikt kan medføre straffeansvar
- brudd på taushetsplikt kan få følger for ansettelses – eller oppdragsforholdet
- taushetsplikten gjelder også etter at ansettelses– eller oppdragsforholdet er avsluttet

Sted/Dato		
Fødselsdato:	Signatur	Navn med blokkbokstaver

Hovedkontor

Middelthunsgate 29
Postboks 5091, Majorstuen
0301 OSLO

Region Midt-Norge

Vestre Rosten 81
7075 TILLER
Telefon: 72 89 65 50

Region Nord

Kongens gate 14-18
Postboks 394
8505 NARVIK
Telefon: 76 92 33 50

Region Sør

Anton Jenssensgate 7
Postboks 2124
3103 TØNSBERG
Telefon: 33 37 23 00

Region Vest

Naustdalsvn. 1B
Postboks 53
6801 FØRDE
Telefon: 57 83 36 50

Region Øst

Vangsveien 73
Postboks 4223
2307 HAMAR
Telefon: 62 53 63 50

VEDLEGG TIL TAUSHETSERKLÆRINGEN

Sikkerhetsloven

§ 11. Sikkerhetsgradering

Når informasjon må beskyttes av sikkerhetsmessige grunner, skal en av følgende sikkerhetsgrader benyttes:

- a. STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- b. HEMMELIG nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- c. KONFIDENSIELT nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- d. BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

Den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon, skal sørge for at informasjonen merkes med aktuell sikkerhetsgrad. Sikkerhetsgradering skal ikke skje i større utstrekning enn strengt nødvendig, og det skal ikke brukes høyere sikkerhetsgrad enn nødvendig.

Sikkerhetsgradering skal ikke gis virkning for lengre tid enn det som er strengt nødvendig, og graderingen skal senest bortfalle etter 30 år. Nærmere regler om ned- og avgradering gis av Kongen. Kongen kan for særskilte tilfeller fastsette unntak fra 30 års regelen i første punktum.

Kongen kan under forutsetning om gjensidighet treffe overenskomst med fremmed stat eller internasjonal organisasjon om sikkerhetsgradering av mottatt informasjon som er sikkerhetsgradert av vedkommende stat eller internasjonale organisasjon, og om plikt til å treffe tiltak for å sikre slik informasjon.

§ 12. Plikt til å beskytte sikkerhetsgradert informasjon

Enhver som får tilgang til sikkerhetsgradert informasjon som ledd i arbeid, oppdrag eller verv for en virksomhet, plikter å hindre at uvedkommende får kjennskap til informasjonen. Taushetsplikten gjelder også etter at vedkommende har avsluttet arbeidet, oppdraget eller vervet. Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov for tilgang til den. Taushetsplikten er likevel ikke til hinder for at sikkerhetsgradert informasjon blir gitt til andre når dette har særskilt hjemmel i lov eller i generell forskrift fastsatt av Kongen.

Kongen gir nærmere regler om håndteringen av sikkerhetsgradert informasjon, herunder om journalisering, oppbevaring, forsendelse og tilintetgjøring. Kongen kan også gi regler om plikt til å legge forholdene til rette for at sikkerhetsgradert informasjon er korrekt, fullstendig og tilgjengelig.

Energiloven

§ 9-3. (Informasjonssikkerhet)

Alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon.

Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.

Departementet kan gi nærmere forskrifter om informasjonssikkerhet i kraftforsyningen og om taushetsplikten.

Beredskapsforskriften

§ 6-2. Sensitiv informasjon

Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.

Med sensitiv informasjon menes spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen, herunder:

- a. Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvedlig hjelpeutstyr som samband.
- b. Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg.
- c. Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.
- d. Oversikt over fordelingsnett til samfunnskritiske funksjoner.
- e. Nøyaktig kartfesting av jordkabler.
- f. Forebyggende sikkerhetstiltak mot bevisst skadeverk.
- g. Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.
- h. Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.
- i. Beredskapsplaner for å håndtere bevisst skadeverk.
- j. Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk.

§ 6-3. Beskyttelse, avskjerming og tilgangskontroll

Alle KBO-enheter skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for sensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.

System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.

Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese sensitiv informasjon.

Damsikkerhetsforskriften

§ 7-8. Informasjonssikkerhet

For vassdragsanlegg i konsekvensklasse 2, 3 og 4 skal det foretas en helhetlig risikovurdering knyttet til all behandling av informasjon om vassdragsanlegget. Som sensitiv informasjon regnes spesifikk informasjon og inngående kjennskap om vassdragsanlegget som kan brukes til å skade anlegget eller påvirke funksjoner som har betydning for sikkerheten. Det skal identifiseres hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming av sensitiv informasjon og gjennomføres tilgangskontroll slik at kun rettmessige brukere får tilgang. Enhver som omfattes av forskriften her plikter å hindre at

andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om vassdragsanlegget. Slik informasjon er å anse som taushetsbelagt informasjon unntatt fra innsyn etter offentleglova § 13. All kommunikasjon og behandling av sensitiv informasjon skal beskyttes mot avlytting og manipulering fra uvedkommende

En sikkerhetsinstruks for å ivareta informasjonssikkerheten skal utarbeides. Det skal gjennomføres tiltak for å ivareta krav etter instruksen.

NVE kan treffe vedtak om at informasjon om vassdragsanlegg skal behandles i henhold til bestemmelsene i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

Offentleglova (når relevant)

§ 13. Opplysninger som er underlagde teieplikt

Opplysninger som er underlagde teieplikt i lov eller i medhald av lov, er unnatekne frå innsyn.

Føresegnene i forvaltningsloven om teieplikt gir sjølvstendige rettssubjekt som er nemnde i § 2 første ledd bokstav c eller d i lova her, høve til å gjere unntak for dokument og opplysninger i same omfang som dei gir forvaltningsorgan det.

Gjeld innsynskravet eit dokument som inneheld opplysningar som er underlagde teieplikt, og denne plikta fell bort dersom den som har krav på tystnad samtykkjer, skal innsynskravet saman med ei eventuell grunngiving på oppmoding leggjast fram for vedkommande med ein høveleg frist til å svare. Svarar vedkommande ikkje, skal dette reknast som nekting av samtykke.

Forvaltningsloven (når relevant)

§ 13. (taushetsplikt).

Enhver som utfører tjeneste eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:

- 1) noens personlige forhold, eller
- 2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningen angår.

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal reknes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes personlige status for øvrig, samt om vilkårene for å gi slike opplysninger.

Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre.

§ 13a. (begrensninger i taushetsplikten når det ikke er behov for beskyttelse).

Taushetsplikt etter § 13 er ikke til hinder for:

1. at opplysninger gjøres kjent for dem som de direkte gjelder, eller for andre i den utstrekning de som har krav på taushet samtykker,
2. at opplysningene brukes når behovet for beskyttelse må anses varetatt ved at de gis i statistisk form eller ved at individualiserende kjennetegn utelates på annen måte, og
3. at opplysningene brukes når ingen berettiget interesse tilsier at de holdes hemmelig, f.eks. når de er alminnelig kjent eller alminnelig tilgjengelig andre steder.

4. at opplysninger om en navngitt domfelt eller botlagt er benådet eller ikke og hvilke reaksjoner vedkommende eventuelt blir benådet til, gjøres kjent.

§ 13b. (begrensninger av taushetsplikten ut fra private eller offentlige interesser).

Taushetsplikt etter § 13 er ikke til hinder for:

1. at opplysningene i en sak gjøres kjent for sakens parter eller deres representanter,
2. at opplysningene brukes for å oppnå det formål de er gitt eller innhentet for, bl.a. kan brukes i forbindelse med saksforberedelse, avgjørelse, gjennomføring av avgjørelsen, oppfølging og kontroll,
3. at opplysningene er tilgjengelig for andre tjenestemenn innen organet eller etaten i den utstrekning som trengs for en hensiktsmessig arbeids- og arkivordning, bl.a. til bruk ved vegledning i andre saker,
4. at opplysningene brukes for statistisk bearbeiding, utrednings- og planleggingsoppgaver, eller i forbindelse med revisjon eller annen form for kontroll med forvaltningen,
5. at forvaltningsorganet gir andre forvaltningsorganer opplysninger om en persons forbindelse med organet og om avgjørelser som er truffet og ellers slike opplysninger som det er nødvendig å gi for å fremme avgiverorganets oppgaver etter lov, instruks eller oppnevningssgrunnlag,
6. at forvaltningsorganet anmelder eller gir opplysninger (jfr. også nr. 5) om lovbrudd til påtalemyndigheten eller vedkommende kontrollmyndighet, når det finnes ønskelig av allmenne omsyn eller forfølgning av lovbruddet har naturlig sammenheng med angiverorganets1 oppgaver,
7. at forvaltningsorganet gir et annet forvaltningsorgan opplysninger (samordning) som forutsatt i lov om Oppgaveregisteret,
8. at forvaltningsorganet gir et forvaltningsorgan i en annen EØS-stat opplysninger som forutsatt i tjenesteloven.

Part eller partsrepresentant som blir gjort kjent med opplysninger etter første ledd nr. 1, kan bare bruke opplysningene i den utstrekning det er nødvendig for å vareta partens tarv i saken. Forvaltningsorganet skal gjøre ham merksam på dette. Likeledes kan forvaltningsorganet pålegge taushetsplikt når vitner o.l. får opplysninger undergitt taushetsplikt i forbindelse med at de uttaler seg til organet. Overtreding av taushetsplikt etter dette ledd kan straffes etter straffelovens § 121, dersom vedkommende er gjort merksam på at overtreding kan få slik følge.

§ 13c. (informasjon om taushetsplikt, oppbevaring av opplysninger undergitt taushetsplikt).

Vedkommende forvaltningsorgan skal sørge for at taushetsplikten blir kjent for dem den gjelder, og kan kreve skriftlig erklæring om at de kjenner og vil respektere reglene.

Dokumenter og annet materiale som inneholder opplysninger undergitt taushetsplikt, skal forvaltningsorganet oppbevare på betryggende måte.

Kongen kan gi nærmere regler om oppbevaring av dokumenter og annet materiale som er undergitt taushetsplikt, om tilintetgjøring av dokumenter eller materiale og om bortfall av taushetsplikt etter en viss tid. Taushetsplikten bortfaller etter 60 år når ikke annet er bestemt i medhold av foregående punktum.

§ 13d. (opplysninger til bruk for forskning).

Når det finnes rimelig og ikke medfører uforholdsmessig ulempe for andre interesser, kan departementet bestemme at et forvaltningsorgan kan eller skal gi opplysninger til bruk for forskning, og at dette skal skje uten hinder av organets taushetsplikt etter § 13.

Til vedtak som nevnt i første ledd kan det knyttes vilkår. Disse kan bl.a. gi bestemmelser om hvem som skal ha ansvar for opplysningene og hvem som skal ha adgang til dem, om oppbevaring og tilbakelevering av utlånt materiale, om tilintetgjøring av avskrifter, om hvorvidt forskerne skal ha adgang til å henvende seg til eller innhente nærmere opplysninger om dem det er gitt opplysninger om, og om bruken av opplysningene for øvrig.

Kongen kan gi nærmere forskrifter om vedtak etter denne paragraf.

§ 13e. (forskeres taushetsplikt).

Enhver som utfører tjeneste eller arbeid i forbindelse med en forskingsoppgave som et forvaltningsorgan har støttet, godkjent eller gitt opplysninger undergitt taushetsplikt til, plikter å hindre at andre får adgang eller kjennskap til:

1. opplysninger undergitt taushetsplikt som forskeren får fra et forvaltningsorgan,
2. opplysninger som i forbindelse med forskningsarbeidet er mottatt fra private under taushetsløfte, og
3. opplysninger som gjelder personer som står i et avhengighetsforhold til den instans (skole, sykehus, anstalt, bedrift, offentlig myndighet m.m.) som har formidlet deres kontakt med forskeren.

Opplysningene kan bare brukes slik det er nødvendig for forskningsarbeidet og i samsvar med de vilkår som måtte være fastsatt etter § 13 d annet ledd. Skal resultater av forskningsarbeidet publiseres eller brukes på annen måte, gjelder § 13 a nr. 1 og 2 tilsvarende.

Brudd på taushetsplikten eller på vilkår etter § 13 d annet ledd, straffes etter straffelovens § 121. Departementet eller vedkommende forvaltningsorgan skal gjøre forskeren og hans medarbeidere kjent med taushetsplikten og straffebestemmelsen, jfr. også § 13 c første ledd.

§ 13f. (bestemmelser om taushets- og opplysningsplikt m.m. i andre lover).

Dersom noen som utfører tjeneste eller arbeid for et forvaltningsorgan, er pålagt taushetsplikt ved bestemmelse i annen lov, forskrift eller instruks av hensyn til private interesser, gjelder §§ 13 til 13 e som utfyllende regler når ikke annet er bestemt i lov eller i medhold av lov.

Bestemmelse i annen lov om rett eller plikt til å gi opplysninger begrenser ikke lovbestemt taushetsplikt, med mindre vedkommende bestemmelse fastsetter eller klart forutsetter at taushetsplikten ikke skal gjelde.

Vedlegg 4

Informasjonssikkerhetsavtale for sensitiv informasjon om energiforsyningen

Parter:

Norges vassdrags- og energidirektorat

Organisasjonsnummer

(NVE)

(Navn på KBO-enhet)

.....

organisasjonsnummer

(Selskapet)

(Virksomhet avtalen inngås med)

1 Innledende bestemmelser

1.1 Bakgrunn og formål med avtalen

NVE (navn på KBO-enhet) er som beredskapsmyndighet del av KBO.. **NVE** har data som er omfattet av taushetsplikten etter lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.

(energiloven) av 29. juni 1990 nr. 50 § 9-3 og forskrift om forebyggende sikkerhet og beredskap i energiforsyning (beredskapsforskriften) av 7. desember 2012 nr. 1157 kapittel 6 (kravene til informasjonssikkerhet). Kravene til informasjonssikkerhet er inntatt i vedlegg 1.

Etter beredskapsforskriften har **NVE** adgang til å gi andre som ikke er KBO-enhet, tilgang til sensitiv informasjon om energiforsyningen såfremt vedkommende vurderes av **NVE** å ha et rettmessig behov for tilgang til slik informasjon.

Denne avtalen er inngått mellom NVE og Selskapet i forbindelse med at:
Selskapet er leverandør av(spesifiser oppdrag) til **NVE**.

Avtalen har som formål å sikre at kravene til informasjonssikkerhet etterleves. Avtalen gjør ingen endring i at både **NVE** og Selskapet skal etterleve den taushetsplikten som etter energiloven § 9-3 er pålagt enhver.

1.2 Hva avtalen gjelder

Denne avtalen regulerer tilgang og behandling av den informasjon som etter beredskapsforskriften § 6-2 er sensitiv informasjon om energiforsyningen og som **NVE** gir tilgang til ved denne avtalen. Informasjonen og hvordan det gis tilgang er spesifisert i vedlegg 2.

2 Partenes plikter og rettigheter

2.1 Selskapet

Selskapet skal:

- 1) Etterleve de til hver tid gjeldende kravene til informasjonssikkerhet. Vedlegg 1 angir kravene til informasjonssikkerhet slik de lyder ved inngåelsen av avtalen.
- 2) Sørge for å holde seg oppdatert på endringer i kravene til informasjonssikkerhet etter energiloven eller beredskapsforskriften.
- 3) Utarbeide en sikkerhetsinstruks og praktisere i samsvar med beredskapsforskriften § 6-4 første ledd.
- 4) Utarbeide en taushetserklæring som skal undertegnes av ansatte i Selskapet som kan få tilgang til informasjonen spesifisert i vedlegg 2. Dersom Selskapet har gitt samtykke til at annet personell i Selskapet kan få tilgang til informasjon spesifisert i vedlegg 2 i forbindelse med oppdraget omfattet av denne avtalen, skal også disse undertegne taushetserklæringen.

- 5) Bruke den informasjon det er gitt tilgang til gjennom denne avtalen kun for utføring av oppdraget spesifisert i pkt. 1.1.
- 6) Sørge for at ansatte i Selskapet og eventuelle annet personell i Selskapet det er gitt samtykke til at får tilgang til informasjonen spesifisert i vedlegg 2 ikke lagrer noen del av denne informasjon på sitt personlige datautstyr eller annet lagringsmedium.
- 7) Ikke skriftlig eller muntlig videreformidle den informasjon det er gitt tilgang til gjennom denne avtalen til andre i Selskapet, tredjepart, inkludert konsulenter, målgrupper for markedsføring eller media, samt eventuelle underleverandører, uten at NVE på forhånd har gitt skriftlig samtykke til at også disse vurderes å ha et rettmessig behov for tilgang ved videreformidling.
- 8) Etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for den informasjon det er gitt tilgang til gjennom denne avtalen i samsvar med beredskapsforskriften § 6-1 og § 6-3.
- 9) Ved avslutning av oppdraget omfattet av denne avtalen levere tilbake informasjonen spesifisert i vedlegg 2. Alle sikkerhetskopier mv. skal slettes fra Selskapets datamaskiner, servere eller annet lagringsmedium.
- 10) Informere NVE skriftlig og på forhånd om enhver endring i Selskapet som har betydning for oppfyllelse av Selskapets plikter etter denne avtalen, for eksempel endring av firmanavn, daglig leder eller lokaler/sted for Selskapets virksomhet.
- 11) Før en eventuell gjeldsforhandling eller konkurs i Selskapet, skal NVE informeres skriftlig. Denne avtalen kan ved slike omstendigheter terminere denne avtalen uten nærmere begrunnelse.

NVE skal:

- 1) Overlevere informasjonen spesifisert i vedlegg 2.
- 2) Informere Selskapet skriftlig ved endringer i kravene til informasjonssikkerhet etter energiloven eller beredskapsforskriften.
- 3) Ha rett til å føre tilsyn med etterlevelsen av bestemmelsene om informasjonssikkerhet, jf beredskapsforskriften § 6-5.

3 Avsluttende bestemmelser

- 3.1 Ved ethvert brudd på kravene til informasjonssikkerhet vil NVE bruke de til enhver tid gjeldende reaksjonsmidler etter energiloven og beredskapsforskriften, samt eventuelt heve avtalen eller kreve erstatning.
- 3.2 Denne avtalen gjelder tilgang og behandling av informasjonen spesifisert i vedlegg 2 inntil oppdraget spesifisert i pkt. 1.1 er avsluttet eller senest ... (dato).

- 3.3 Avtalen trer i kraft når begge parter har undertegnet den.
- 3.4 Denne avtalen gjelder inntil den blir sagt opp av én av partene med 30 kalenderdagers skriftlig varsel.
- 3.5 Endringer og/eller tillegg til denne avtalen skal være skriftlige og skal være undertegnet av begge parter.

Denne avtalen er utferdiget i to eksemplarer, ett til hver av partene.

Dato:

Dato:

.....
NVE

.....
Selskapet

Vedlegg 5



Varsling etter bfe §2-6 - SITUASJONSRAPPORT - (skjema v.03.06.2013)

Til:	(Virksomhet, avdeling, kriseledelsen)	(tlf, faksnr, e-post)
Fra:	(Virksomhet, avdeling, kriseledelsen, <u>kontaktperson</u>)	(tlf, faksnr, e-post)
Rapport nr:	(evt saksnr)	(sted og dato)
Sensitiv eller åpne rapport?	Ved kryss ☐ er rapporten Underlagt taushetsplikt etter energiloven § 9-3 jf beredskapsforskriften (bfe) § 6-2. Unntatt fra innsyn etter offentleglova § 13.	

1. Hva foregår a) Hva har skjedd? b) Hvor mange er berørt? c) Hvilke områder (kommuner er berørt)? d) Antatt varighet? e) Konsekvenser for virksomhet og samfunn? f) Annet?	(tekst)
2. Tiltak vi har iverksatt a) Retting/sikring b) Ressurser c) Publikumsinfo d) Annet..	(tekst)
3. Tiltak som vurderes a) Økt beredskap/rekvirere ressurser b) annet	(tekst)
4. Etablert kriseledelse a) Også hvorvidt etablert kontakt med andre kriseledelser i og utenfor KBO? b) annet	(tekst)
5. Udekkede behov a) Forhold virksomheten har uløst? b) Trenger bistand?	(tekst)
6. Merknader a) Særlig forhold som KDS/NVE bør være kjent med b) Forventet utvikling over tid (kommende døgn)... c) Annet relevant	(tekst)
7. Vedlegg	(spesifiser)

Varsling etter bfe §2-6 - SITUASJONSRAPPORT - (skjema v.03.06.2013)



Skrevet av:	Godkjent av:
Filnavn:	

Kopi:	(Virksomhet, avdeling, kriseledelse)	(tlf/faksnr/e-post)	Vedlegg:	1 (spesifiser)
	(Virksomhet, avdeling, kriseledelse)	(tlf/faksnr/e-post)		2 (spesifiser)
	(Virksomhet, avdeling, kriseledelse)	(tlf/faksnr/e-post)		3 (spesifiser)
	(Virksomhet, avdeling, kriseledelse)	(tlf/faksnr/e-post)		4 (spesifiser)

Når og hva som skal varsles og rapporters fremgår av bestemmelsen i Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).

Plikten er todel:

- 1) Varsle umiddelbart til NVE ved ekstraordinære hendeler (strøøre strømbrydd, akutte trusler mot forsyningssikkerheten mv,
- 2) rapportere i ettertid om uønskede hendelser jfr

- a. Forsøk på inntrengning og/eller manipulasjon av hele eller deler av driftskontrollsystemet og avanserte måle- og styringssystem (AMS).
- b. Innbrudd, hærværk, sabotasje eller andre kriminelle handlinger, eller forsøk på dette.
- c. Mistanke om adferd ved viktige anlegg av betydning for energiforsyningen.
- d. Situasjoner hvor sensitiv informasjon om kraftforsyningen er blitt kjent for andre enn rettmessige brukere, eller mistanke om dette.
- e. Avbrudd i distribusjon av elektrisitet i mer enn to timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere.
- f. Avbrudd i fjernvarmeforsyningen i mer enn 12 timer som berører viktige samfunnsfunksjoner eller et stort antall sluttbrukere.
- g. Større havarier i sentral- og regionalnettet.
- h. Omfattende feil og sikkerhetstruende hendelser i driftskontrollsystemer.

Dette skjemaet er for varsler. Et eget og mer detaljert skjema for etterskuddsvis rapporter er tilgjengelig på www.nve.no

Sensitiv informasjon

Sensitiv informasjon skal håndteres i tråd med bestemmelsene i beredskapsforskriften § 6-2.

- Det gjelder også dette skjemaet når det er utfyllt og evt inneholder sensitiv informasjon.

Varsler og rapporter sendes hit:

- beredskapsrapportering@nve.no
- PS: For rapportering etter denne bestemmelsen ligger det tilgjengelig egne rapporteringsskjema på www.nve.no

Ved særlige ekstraordinære forhold utenom normal kontortid skal KBO-enheten også varsle pr telefon til:

- NVEs flomvarsling og døgnapne beredskapstelefon
- 22 95 93 60 og 909 92 231

Vedlegg 6

Hendelser forårsaket av teknisk svikt, uhell, ulykker, naturgitte forhold osv.

Side 1 av 2

Enhetens/selskapets navn:									
Adresse:				Postnr.:		Poststed:			
Telefon:		Telefaks:		E-post:					
Leder:				Beredskapsleder:					
Beredskapskoordinator:									
Tids- og stedsangivelse for hendelsen:				Dato:		Kl.		Rapport nr:	
Fylke:			Stedsnavn:						
By		Tettsted		Landsbygd	Annet:				
Type hendelse:		Ulykke / uhell, hva:							
Teknisk svikt				Naturgitte forhold					
	Slitasje		Mekanisk svikt		Tordenvær		Vann/nedbør		Vegetasjon
	Varmgang		Elektrisk feil		Vind		Flom		Ras
	Materielltrethet		Korrosjon		Snø/is		Forurensing		Brann
	Annet:				Fugl/dyr		Annet:		
Medvirkende årsak(er):									
Mennesker		Driftspåkjenning			Konstruksjon/montasje				
	Eget personale		Overbelastning		Konstruksjonsfeil				
	Innleid		Høy/lav spenning		Produksjonsfeil				
	Andre		Høy/lav frekvens		Montasjefeil				
	Feilbetjening		Produksjonsutfall		Feil innstilling/justering				
	Trefelling		Annet:		Annet:				
	Anleggsarbeid	Drift / vedlikehold:							
	Trafikkskade		Mangelfullt vedlikehold		Mangelfulle avtaler				
Annet:			Manglende instruks/rutiner		Annet:				
Konsekvenser av hendelsen:									
Produksjon:		Overføring/fordeling							
	Stopp		Brudd						
	Innskrenkning		Innskrenkning						
Annet:									
Økonomiske konsekvenser av hendelsen:									
Produksjonstap, ca kr.:				Materielle kostnader, ca. kr.:					
KILE-kostnader, ca kr.:				Arbeidskostnader, ca. kr.:					
Annet:									

Hendelser forårsaket av teknisk svikt, uhell, ulykker, naturgitte forhold osv.

Side 2 av 2

Objekt(er) som ble rammet av hendelsen:									
Produksjonsanlegg:			Nett:				Stasjoner tilknyttet:		
Vannkraft			Sentralnett		Gass		Sentralnett		
Kraftstasjon			Regionalnett		Fjernvarme		Regionalnett		
Rørgate			Distribusjonsnett		Annet:		Distribusjonsnett		
Dam			300 – 400 kV				300 – 400 kV		
Vindkraft			132 – 220 kV				132 – 220 kV		
Biobrensel			32 – 66 kV				32 – 66 kV		
Gass			>1 – 22 kV				>1 – 22 kV		
Fjernvarme / annet			Lavspenning				Trafostasjon		
			Luftnett				Koblingsstasjon		
			Kabelnett				Annet:		
Adm. bygning:			Øvrige bygg:				Driftssentral:		
Kontor			Verksted		Garasje		Sentralnett		Distribusjonsnett
Datarom			Lager		Innhegning		Regionalnett		Kraftstasjon
Annet:			Annet:				Annet		
Feilbeskrivelse:									
Mekanisk feil		Materiellteknisk feil			Elektrisk feil		Annet:		
Utløsende årsak:									
Analyse / vurdering:									
Kortfattet beskrivelse av det inntrufne:									
Kortfattet beskrivelse av forebyggende tiltak som er/var gjennomført:									
Kortfattet beskrivelse av selskapets evne til å håndtere det inntrufne (administrativt, intern og eksternt info. osv.):									
Kortfattet beskrivelse av gjenopprettingstiltak og selskapets evne til å gjenopprette funksjonalitet/utbedre skader (tilgang til personell, kompetanse, materiell, utstyr, osv.):									
Kortfattet beskrivelse av samfunns- og selskapsmessige konsekvenser på grunn av det inntrufne:									
Sted:			Dato:			Signatur:		Antall vedlegg:	

Vedlegg 7

Hendelser forårsaket av uvedkommende

(Side 1 av 2)

Enhetens/selskapets navn:									
Adresse:				Postnr.:		Poststed:			
Telefon:		Telefaks:		E-post:					
Daglig leder:				Beredskapsleder:					
Beredskapskoordinator:									
Tids- og stedsangivelse for hendelsen:				Dato:		Kl.		Rapport nr:	
Fylke:			Stedsnavn:						
By	Tettsted	Landsbygd	Annet:						
Type hendelse(er):									
Vinningsforbrytelse	Ja	Nei	Vet ikke	Bevisst handling	Ja	Nei	Vet ikke		
Inntrengning:		Skadeverk:		Hacking		Manipulering:			
Innbruddsforsøk		Hærverk		Vellykket inntregning		Bestikkelser			
Innbrudd		Brann		Mislykket inntregning		Trusler			
Mistenkelig nærvær		Sabotasje		Adm. system		Avlytting			
Fotografering		Terror		Driftskontr.system		Uvanlig utspørring			
Annet:		Annet:		Annet:		Annet:			
Tap og evt. konsekvenser av hendelsen:									
Tap av informasjon:		Materielle tap:				Konsekvenser:			
Driftssensitiv		PC		Materiell		Fysisk skade			
Adm./øk.sensitiv		Programvare		Hva:		Ca. kostnad:			
Personalsensitiv		Hva:		Utstyr		Ukjent omfang			
Annet:		Kommunikasjonsutstyr		Hva:		Strømutfall			
		Hva:		Annet:		Annet:			
Objekt(er) som ble rammet av hendelsen:									
Produksjonsanlegg:		Nett:				Stasjoner tilknyttet:			
Vannkraft		Sentralnett		Gass		Sentralnett			
Kraftstasjon		Regionalnett		Fjernvarme		Regionalnett			
Rørgate		Distribusjonsnett		Annet:		Distribusjonsnett			
Dam		300 – 400 kV				300 – 400 kV			
Vindkraft		132 – 220 kV				132 – 220 kV			
Biobrensel		32 – 66 kV				32 – 66 kV			
Gass		>1 – 22 kV				>1 – 22 kV			
Fjernvarme / annet		Lavspenning				Trafostasjon			
		Luftnett				Koblingsstasjon			
		Kabelnett				Annet:			
Adm. bygning:		Øvrige bygg:		Driftsentral:					
Kontor		Verksted		Garasje		Sentralnett		Distribusjonsnett	
Datarom		Lager		Innhegning		Regionalnett		Kraftstasjon	
Annet:		Annet:		Annet					

Hendelser forårsaket av uvedkommende

(Side 2 av 2)

Anmeldelse og observasjoner:				Er hendelsen meldt til politi / lensmann:				☐	Ja	☐	Nei
Identiteten til den / de som forårsaket hendelsen (dersom kjent):											
Navn:				Alder / Id:				Adresse:			
Utro tjener:		☐	Ja	☐	Nei	☐	Vet ikke	☐	Mistanke		
Evt. andre opplysninger (biltype, antall personer, antatt alder, andre kjennetegn, mm.):											
Analyse / vurdering:											
Kortfattet beskrivelse av det inntrufne:											
Kortfattet beskrivelse av forebyggende tiltak som er/var gjennomført (fysisk sikring, overvåking, mm.):											
Kortfattet beskrivelse av selskapets evne til å håndtere det inntrufne (administrativt, intern og eksternt info mm):											
Kortfattet beskrivelse av gjenopprettingstiltak og selskapets evne til å gjenopprette funksjonalitet / utbedre skader (tilgang til mannskap, kompetanse, materiell, utstyr, osv):											
Kortfattet beskrivelse av eventuelle samfunns- og selskapsmessige konsekvenser pga. det inntrufne:											

Underlagt taushetsplikt etter energiloven § 9-3 jf bfe § 6-2.

Unntatt fra innsyn etter offentleglova § 13.

Sted:	Dato:	Signatur:	Antall vedlegg:
-------	-------	-----------	-----------------

**Underlagt taushetsplikt etter energiloven § 9-3 jf bfe
§ 6-2.**

Unntatt fra innsyn etter offentleglova § 13.

Vedlegg 8



Tilgang av personell som dekker kritisk funksjon i sivil krigstidsoppsetning (SKOP) i Fritaksordningen

Om sivil krigstidsoppsetning (SKOP)	
Navn på SKOP:	Organisasjonsnummer til SKOP:
Navn til rapporterende ledd (RL) som SKOP tilhører:	Organisasjonsnummer til rapporterende ledd (RL) som SKOP tilhører:

Tilgang av person som dekker kritisk funksjon i SKOP	
Navn:	Fødselsnummer (11 siffer):
Innkalt til tjeneste ved (avdeling):	Fremmøtetidspunkt:

Om den kritiske funksjonen i SKOP		
Stilling/funksjon ved SKOP:	Antall som må dekke samme funksjon:	Antall som kan dekke samme funksjon:
Begrunnelse for tilgangen, hvorfor funksjonen er kritisk for virksomheten, henvisning til beredskapsplaner (Skal fylles ut av SKOP):		

Erklæring
Det bekreftes at personen det søkes fritak for dekker en funksjon som er kritisk for å opprettholde driften i virksomheten. Virksomheten inngår i beredskapsplanene til RL, eller er definert som samfunnskritisk virksomhet av RL. Det bekreftes at virksomheten ikke har andre personer som kan dekke denne funksjonen ved krise, konflikt eller krig, og at det ikke er mulig å lære opp andre personer innen rimelig tid. Jeg er inneforstått med at det kan medføre straffeansvar å gi uriktige opplysninger som fører til at noen unndrar seg tjeneste i Forsvaret, jf. vernepliktsloven §§ 48 og 49.

Kontaktperson ved SKOP		
Navn:	Stilling:	Telefon:
Postadresse:	Besøksadresse:	
E-postadresse:	Sted, dato:	Underskrift:

Forutsetninger og vilkår for fritak for fremmøte i Forsvaret finnes på baksiden av dette skjemaet.

Skjemaet sendes til

Vernepliktsverket
Postboks 800, postmottak
2617 LILLEHAMMER

Telefaks: 61 10 36 99
E-post: forsvaret@mil.no

Forutsetninger og vilkår for fritak for fremmøte i Forsvaret ved krise, konflikt eller krig (Fritaksordningen)

1 Forutsetningene for at det gis fritak for fremmøte i Forsvaret er at

- virksomheten dekker en samfunnskritisk funksjon, og er registrert som SKOP,
- arbeidstakeren dekker en kritisk funksjon i virksomheten,
- arbeidstakeren har fullført førstegangstjenesten og
- arbeidstakeren er disponert eller planlagt disponert i Forsvarets styrker, Heimvernet inkludert, har fått brev om nytilføring til Heimvernet eller er innkalt til repetisjons-/hjelpetjeneste.

Alle kriteriene må være oppfylt før det er aktuelt å overføre personell til fritaksordningen.

2 Hovedpunkter i forhold til praktiseringen av ordningen fram til nye forskriftsbestemmelser er vedtatt:

- Departementene har ansvaret for å melde om tilgang for nye rapporterende ledd (RL) i ordningen, samt melde om avgang dersom RL skal ut av ordningen. Skjema for tilgang/avgang av RL finnes på nettsiden
- RL har ansvaret for å melde om tilgang for nye sivile krigstidsoppsetninger (SKOP) i ordningen, samt melde om avgang dersom SKOP skal ut av ordningen. Skjema for tilgang/avgang av SKOP finnes på nettsiden.
- SKOP har ansvaret for å melde om tilgang i ordningen for personer som dekker samfunnskritiske funksjoner, samt melde om avgang dersom personer skal ut av ordningen. Skjema for tilgang for personer som dekker samfunnskritiske funksjoner finnes på nettsiden.
VPV gjør oppmerksom på at personell som er disponert i Heimvernet og som har fått innkalling til årlig trening først kan bli overført til fritaksordningen fra neste mobiliseringstermin. Dette innebærer at vedkommende må møte til årets trening i henhold til mottatt innkalling.
- Dersom en søknad om fritak blir avslått, kan SKOP klage på avgjørelsen. Skjema for klage på avslag i fritaksordningen finnes på nettsiden www.forsvaret.no/verneplikt.

3 Følgende forhold gir grunn for avslag på søknad:

Omfattes ikke av fritaksordningen

- Virksomheten er ikke registrert som SKOP*
Virksomheter som ikke er fastsatt som SKOP av RL, omfattes ikke av fritaksordningen.
- Ikke øvd vernepliktig*
Personer som ikke er øvde vernepliktige omfattes ikke av fritaksordningen.
- Personell overført til Sivildforsvaret eller Politireserven*
Personell som er overført til Sivildforsvaret eller Politireserven omfattes ikke av fritaksordningen.

Unntatt fra reglene om fritak

- Registrert som ansatt i Forsvaret*
Fast ansatte i Forsvaret er unntatt fra reglene om fritak. Dette gjelder alle typer tilsettingsforhold i Forsvaret.
- Registrert med en kompetanse Forsvaret ikke kan unnvære*
Personer som innehar en kompetanse som Forsvaret ikke kan unnvære, kan unntas fra reglene om fritak. Unntaket skal bare benyttes dersom personer med tilsvarende kompetanse ikke er tilgjengelig. Personer som er gitt militærmedisinsk utdanning av Forsvaret, er normalt unntatt fra reglene om fritak.
- Registrert som fartøysbefal i Sjøheimvernet*
Personer med navigatør- eller maskinistutdanning som er utdannet som befal i Sjøheimvernet er unntatt fra reglene om fritak.
- Registrert som områdesjef i Heimvernet*
Personer som er registrert som områdesjef i Heimvernet er unntatt fra reglene om fritak så lenge dette verv innehas.
- Registrert med kontrakt med Forsvaret*
Personer som har inngått kontrakt med Forsvaret er unntatt fra reglene om fritak for kontraktens varighet.
- Registrert som polititjenesteperson på Forsvarets kvote*
Personer som etter avtale med Politidirektoratet er øremerket spesielle stillinger i Forsvaret er unntatt fra reglene om fritak.

Vedlegg 9



Om sivil krigstidsoppsetning (SKOP)	
Navn på SKOP:	Organisasjonsnummer til SKOP:
Navn til rapporterende ledd (RL) som SKOP tilhører:	Organisasjonsnummer til rapporterende ledd (RL) som SKOP tilhører:

Klagen gjelder for		
Navn:	Fødselsnummer (11 siffer):	
Innkalt til tjeneste ved (avdeling):	Fremmøtetidspunkt:	
Stilling/funksjon ved SKOP:	Antall som må dekke samme funksjon:	Antall som kan dekke samme funksjon:

Årsaken til klagen (Bruk baksiden om nødvendig)

Kontaktperson ved SKOP		
Navn:	Stilling:	Telefon:
Postadresse:	Besøksadresse:	
E-postadresse:	Sted, dato:	Underskrift:

Merknader fra RL anføres på baksiden av skjemaet.

Skjemaet sendes til Vernepliktsverket med gjenpart til RL

Vernepliktsverket
Postboks 800, postmottak
2617 LILLEHAMMER

Telefaks: 61 10 36 99

E-post: forsvaret@mil.no

Merknad fra RL (Skal fylles ut ved klagebehandling)**Kontaktperson ved RL**

Navn:

Stilling:

Telefon:

E-postadresse:

Sted, dato:

Underskrift:

RL skal sende utfylt skjema tilVernepliktsverket
Postboks 4074
2306 HAMAR**Telefaks:** 62 51 58 60**E-post:** vpv.fritaksordningen@mil.no

Vedlegg 10

KBO-enhet (selskapsnavn):	
------------------------------	--

Følgende info henter vi fra Brønnøysundregisteret, brreg.no, dersom det er registrert galt hos oss må det først rettes opp der:

- Postadresse
- Postnummer
- Poststed
- Webside
- E-post til firma
- Orgnr
- Tlf Sentralbord

Følgende info trenger vi fra selskapet direkte:

Beredskap tlf nr:	
Beredskap e-post adr:	
Satellitt tlf:	
KDS-distikt:	

Beredskapsroller:

Rolle	Navn	Dir. tlf. (kontor)	Mobil	E-post
Daglig leder				
Beredskapsleder				
Beredskapskoordinator				
IKT sikkerhets leder				

Vedlegg 11

Forklaring til normer det er henvist til i bfe kapittel 5 (sikringstiltak).

NS-EN 1627 standard for innbrudds-/fasadesikring av dører, porter, vinduer, gitter, sjalusier mv. - er inndelt i 6 sikkerhetsklasser

For høyere krav ("strongrom" og fortifikasjon) gjelder standard NS-EN 1143.

NS-EN 356 standard for sikkerhetsglass - er inndelt i 5 klasser hæververkshemmende og over dette 3 klasser innbruddshemmende

For høyere krav (skuddhemmende) gjelder standard NS-EN 1063.

NS-EN 12320 standard for motstandsdyktighet hos hengellåser og hengellåsbeslag - er inndelt i 6 sikkerhetsklasser *)

NS-EN 1303 standard for motstandsdyktighet hos faste låseenheter med tilbehør - er inndelt i 6 sikkerhetsklasser *)

Før høyere krav (høysikkerhetslåser) standard etter NS-EN 1300.

*) Låser med beslag og hengellåser er alternativt godkjent av "Forsikringsselskapenes Godkjenningnemnd" – **FG** i 5 klasser

Forsvarsbygg som har utarbeidet en omfattende publikasjon ("Sikringshåndboka") for beskyttelse av bygg og anlegg mot kriminalitet henviser til skallsikring (innbruddsikring) i 4 klasser hvor skallsikring 1 tilsvarer overnevnte sikkerhetsklasse 3 opptil skallsikring 4 som tilsvarer sikkerhetsklasse 6.

Denne veiledning til BfK henviser til sikkerhetsklasser i forhold til dette intervallet – dvs. sikkerhetsklasse 2 (helst 3) – 6 i de EN som her er uthøvet.

For enda bedre sikring opererer Forsvarsbygg med såkalt forsterket rom i ytterligere 4 klasser.

Hvor det er aktuelt angir vi i denne veiledningen konkrete bygningstekniske krav og beregningsmåter (f.eks. i cm betong). Vi viser også til:

NS-EN 1992 "Prosjektering av betongkonstruksjoner" – beregnings- og konstruksjonsregler.

NS-EN 1990 "Prosjektering av konstruksjoner" - pålitelighet (jf konsekvenser av konstruksjoners sammenbrudd) - er inndelt i 4 pålitelighetsklasser

NS-EN 13501 Brannmotstand er angitt som følger

Tall som 60, 90 og 120 - den tid i minutter vedkommende bygningsdel skal kunne opprettholde sine funksjoner ved nedennevnte påvirkninger (bokstavkoder):

E – integritet – motstå gjennombrenning

I – isolasjon – hindre spredning ved temperaturøkning på motsatt side av brannen

R – lastbærende funksjon – bygningsdelens (f.eks. vegg eller søyle) evne til å holde konstruksjonen opp under brann

M – mekanisk styrke – bygningsdelens motsand mot slag fra fallende gjenstander ol.

Sammenhengen mellom nye NS-EN standarder og eldre standarder

NS-EN 1627 har erstattet ENV 1627 og tidligere NS 3170 slik at

NS-EN 1627 sikkerhetsklasse 3 tilsvarer NS 3170 sikkerhetsklasse 2

NS-EN 1627 sikkerhetsklasse 4 tilsvarer NS 3170 sikkerhetsklasse 3

osv.

NS-EN 356 har erstattet NS 3217 mv - herunder.

NS-EN 356 hæverkshekkende vindu klasse P2A tilvarer NS 3214 (INSTA 151) A1

NS-EN 356 hæverkshekkende vindu klasse P3A tilvarer NS 3214 (INSTA 151) A2

osv

NS-EN 356 innbruddshekkende vindu klasse P6B tilvarer NS 3215 (INSTA 152) B1

NS-EN 356 innbruddshekkende vindu klasse P7B tilvarer NS 3215 (INSTA 152) B3

osv

FG godkjente vinduer tilsvarer normalt minst innbruddshekkende klasse B1

NS-EN 1303 har erstattet NS 3620 slik at

EN 1303 sikkerhetsklasse 4 tilsvarer NS 3620 sikkerhetsklasse 3

EN 1303 sikkerhetsklasse 5 tilsvarer NS 3620 sikkerhetsklasse 4

osv.

NS-EN 12320 har erstattet SSFN 014

NS-EN 12320 sikkerhetsklasse 3 tilsvarer SSFN 014 sikkerhetsklasse 2

NS-EN 12320 sikkerhetsklasse 4 tilsvarer SSFN 014 sikkerhetsklasse 3

osv.

NS-EN 1992 har erstattet NS 3473

NS-EN 1990 har erstattet NS 3490

NS-EN 13501 har erstattet NS 3919

Vedlegg 12

Sammenhenger mellom sikringsnivå i bfe kapittel 5 og sikringsklasser etter europeiske normer (NS-EN) for ulike elementer i en balansert sikring. Sikringsklasser (mot innbrudd ol.) hvor "motstandsstyrken" er kvantifisert (testkriterier) i form av innbruddstider for ulike verktøy og angrepsmetoder. Dette er så koblet videre til andre elementer i en helhetlig skallsikring og de ulike standarder og klasser som finnes for disse.

NB! Dette er bare eksempler mht. av de mest relevante normer og klasser. For veiledende krav etter bfe § 5-4 til § 5-6 Sikringstiltak (etter klasse).

Bfe sikringsnivå	Låser m/beslag	Hengelåser	Dører, gitter mv.	Vegger ol.			Glass (gml. standard i parentes)		Låser m/beslag
Vedlegg 1 til 3	EN 1303, 12209	EN 12320	EN 1627	tykkelse	kvalitet	armering	EN 356	ca. tykkelse i mm	FG klasse
Normal	sikringsklasse 2 (helst 3)			helstein	murvegg	armert	<u>Hærverkshemmende (laminert)</u> P 5A (A3+) 10		FG 2
				<u>armert betong:</u>			<u>Innbruddshemmende (laminert)</u>		
Middels	sikringsklasse 3			80 mm	B 30	K 189	P6B (B1)	12	FG 2 eller 3
God	sikringsklasse 4			120 mm	B 30	K 257	P7B (B2)	15	FG 3 eller 4
Høy	sikringsklasse 5			150 mm	B 35	K 355	P8B (B3)	18 - 20	FG 4 eller 5
	sikringsklasse 6			200 mm	B 35	K 355	EN 1063		
Eventuelt kraftigere innbruddsikring etter bl.a. EN 1143				osv. jf. konstruksjonskrav etter EN 1990 og EN 1992			<u>Skuddhemmende (multilaminert)</u> BR 2 (C1) c) 19 til 25 d) (Tidligere "RSK" krav operatørrom)		Sikring mot dirking: minimum FG 3
							d) glasstykkelse avhenger av krav til sikring mot splinter/avskalling på innsiden		
De overnvente sikringklasser (eng: "grade") er å anse som minimum							[Skala skuddsikkert fortsetter opp til BR 7 og videre i SG for tyngre våpen]		Denne kolonnen gir kun tilnærmet ekvivalente klasser
Sikringsklasse 1 godtas ikke for anlegg klassifisert etter bfe.									
Normal er mao. her å anse som et minimum									

Merk!

Disse klasser/krav omfatter i utgangspunktet ikke brannsikring. Dette inkludert rømningsveier ol. må vurderes særskilt.
Generelt bør yttervegger og seksjonerende vegger være i brannklasse REI 60 eller bedre, dører mv. i EI 60 eller bedre.

De dimensjoner, kvaliteter mv. som er angitt i denne tabell tar kun hensyn til sikringsmessige krav.

De bygningstekniske mv. krav til konstruksjonen som sådan må beregnes og utføres etter gjeldende regler/normer.

Vedlegg 13

Beredskapsrom – utstyr, drift, vedlikehold og kontroll

Utstyrsliste for beredskapsrom

Følgende utstyr bør være i eller i nærheten (raskt tilgjengelig) av beredskapsrom:

- Sambandsutstyr
- Radio
- Termometer og hygrometer
- Håndlykter
- Brannslukningsutstyr - apparat (pulver) og/eller brannslange
- Førstehjelpsutstyr, stasjonær førstehjelpsenhet
- Sykebåre med 2 ulltepper og annet mobilt førstehjelpsutstyr
- Vannbeholdere/plastkanner med tappekran (20 liter per person, min. 100 liter bærbart)
- Toalett, vaske- og rengjøringsutstyr
- Bord og stoler
- Senger/hvilestoler
- Håndverktøy
- Utbrytningsverktøy bestående av spett, slegge (med reserveskaft), krafse, meisel
- Klosser for underlag for åpning av dører
- Reserve lypærer, sikringer, batterier med mer
- Reservedeler for nødstrømsaggregat (viftreim, pakninger og liknende)
- Personlig utstyr
- Annet enheten finner relevant

Det skal foreligge oppdaterte utstyrslistes, og planer for utstyr som skal bli tilført.

Drift og vedlikehold

Ved de rutinemessige inspeksjonene skal følgende kontrolleres:

Bygningsteknisk:

- Dører, luker og porter
- Vannlekkasjer
- Skader på betong
- Rustangrep på stålkonstruksjoner
- Fuktighetsangrep på trekonstruksjoner

Ventilasjon

- Ventilasjonsanlegg med prøvekjøring av ventilasjonsaggregat. Det kontrolleres at viftene for fredsventilasjon er i orden og at det ikke er ulyder i lagre, motor, vifter, med mer
- Ventiler av alle slag kontrolleres. Om nødvendig foretas demontering og rengjøring og innsetting av alle bevegelige deler og anleggsflater med silikonholdig olje

Sanitærinstallasjoner:

- Tilbakeslagsventiler i drens- og kloakksystemet, samt øvrig sanitærutstyr skal kontrolleres og rengjøres minst en gang hvert år.

Elektroteknisk anlegg:

- Sikringsskap, varmeovner, og belysningsutstyr
- Reserverlager av sikringer, lysstoffrør og liknende kompletteres ved behov
- Nødstrømsanlegg med prøvekjøring av aggregat (minimum 30 minutter med last, se instruksjonsbok)
- Smøring og nødvendig etterfylling av olje og drivstoff
- Batterier

Oppvarming og fuktighet:

- Regulering av elektriske ovner og varmebatteri må skje på grunnlag av erfaring på vedkommende sted
- På grunn av høy relativ fuktighet i sommerhalvåret bør luftmengden som suges inn reduseres mest mulig
- Sjekke at inventar og utstyr er hensiktsmessig lagret og ikke skades av fuktighet.

Kontroll

I tillegg til forannevnte inspeksjoner skal alle beredskapsrom kontrolleres minimum en gang hvert år for følgende:

- Dører, luker og porter - hengsler, vridere, inspeksjonsplugg og pakninger
- Overtrykksmåler prøves ved å åpne og lukke reguleringsventilene når ventilasjonsanlegget er i gang. Ved mistanke om at måleren ikke viser rett, skal denne demonteres og sendes leverandøren for kontroll.
- Sanitærutstyr med drens- og avløps-/kloakkledninger med sjokk og/eller tilbakeslagsventiler (om nødvendig foretas rengjøring)
- Brannsløkkingsutstyr
- Sambandsopplegget, med prøving av utstyr

Når det ved beredskap beordres klargjøring av beredskapsrom, skal enheten gjennomføre fullstendig vedlikeholdsinspeksjon. Blant annet skal enheten funksjonsprøve og kontrollere at tekniske installasjoner virker slik det er forutsatt, og straks utbedre eventuelle mangler.

Spesielt skal enheten:

- Teste sambandsutstyr
- Prøvekjøres ventilasjonsanlegg og nødstrømsaggregat
- Fylle vanntanker
- Vurdere behov for reserveproviant

Vedlegg 14



Underlagt taushetsplikt etter energiloven § 9-3 jf bfe § 6-2.

Unntatt fra innsyn etter offentleglova § 13.

(når utfylt)

Skjema for egen evaluering

Beskyttelse av driftskontrollsystem

Dato for gjennomgang:			
Ansvarlig for gjennomgang:			
Godkjent av:		Dato godkjent:	



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
§ 7-1. Generell plikt til å beskytte driftskontrollsystemet							
7.1.2	Har det blitt utarbeidet styrende mål for beskyttelse av driftskontrollsystem?						
7.1.2	Er ansvarsforholdene knyttet til beskyttelse av driftskontrollsystemet entydig plassert i organisasjonen?						
§ 7-2. Overordnede sikkerhetsregler							
7.2.1	Har virksomheten utarbeidet overordnede sikkerhetskrav for beskyttelse av driftskontrollsystemet?						
7.2.2	Er reglene gjennomgått og godkjent av virksomhetens ledelse?						
7.2.3	Blir det med jevne mellomrom foretatt rapportering om hvorvidt reglene etterfølges til virksomhetens ledelse?						
7.2.4	Er det i virksomhetens virksomhetsplaner lagt inn at reglene skal gjennomgås årlig?						
§ 7-3. Dokumentasjon av driftskontrollsystemet							
7.3.1	Er dokumentasjon av driftskontrollsystemet oppdatert?						
7.3.2	Er det utarbeidet rutiner/prosedyrer/retningslinjer for når dokumentasjonen skal oppdateres?						
7.3.3.a	Er det utarbeidet en skematisk fremstilling av driftskontrollsystemet?						
7.3.3.b	Viser fremstillingen alle hovedkomponenter og sambandet/nettverket som binder driftskontrollsystemet sammen						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.3.3.c	Viser fremstillingen eventuelle tilkoblingspunkter mot Internett eller andre nettverk som ikke inngår i prosessnettverket?						
§ 7-4 Kontroll med brukertilgang							
7.4.2	Er det utarbeidet en ordning, rutine eller prosedyre for å tildele, endre eller slette rettigheter for tilgang til driftskontrollsystemet?						
7.4.3	Er det utpekt en ansvarlig for dette?						
7.4.4	Finnes det en oppdatert oversikt over hvem som har tilgang til hva i driftskontrollsystemet og hvilke funksjoner de har lov til å utføre?						
7.4.5	Utarbeides det logg over hvem som har vært pålogget driftskontrollsystemet og når?						
§ 7-5 Kontroll ved endringer i driftskontrollsystemet							
7.5.1	Er det utarbeidet rutine(r) eller retningslinje(r) for hvordan endringer i driftskontrollsystemet skal foregå?						
7.5.2	Er det vurdert hvilke typer endringer som krever mer oppmerksomhet i form av for eksempel en risikovurdering forut for endringene?						
§ 7-6 Kontroll med utstyr i driftskontrollsystemet							
7.6.1	Har dere kontroll med at utstyr i prosessnett og admnett (eller andre nett) ikke brukes om hverandre?						
7.6.2	Har dere etablert mulighet for kobling mellom prosessnett og annet nett?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.6.3	Er en eventuell sammenkobling sikret på en slik måte at uvedkommende ikke kan utnytte koblingen for å trenge inn i prosessnettet?						
7.6.4	Har dere utarbeidet en liste over vesentlig utstyr i driftskontrollsystemet?						
7.6.5	Har dere et system for merking av utstyret?						
7.6.6	Er det utarbeidet en beskrivelse som forteller hva som er vesentlig utstyr?						
7.6.7	Er det utarbeidet en rutine eller prosedyre som forteller hvordan man skal fjerne all sensitiv informasjon på utstyret før det kasseres, gis bort eller på annen måte avhendes?						
7.6.8	Benyttes det trådløse datanettverk i driftskontrollsystemet (tradisjonell wifi)?						
§ 7-7 Håndtering av feil, sårbarheter og sikkerhetsbrudd							
7.7.1	Har dere etablert prosedyrer for hvordan dere skal agere dersom man oppdager alvorlige hendelser i driftskontrollsystemet?						
7.7.2	Har dere en avtale med systemleverandør, eller etablert andre metoder/ordninger for å fange opp eller få rapporter om eventuelle sårbarheter i viktig programvare som benyttes i driftskontrollsystemet?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.7.3	Har dere egen kompetansen eller inngått avtale med leverandør om bistand ved feil i driftskontrollsystemet? (Gjelder både samband og programvare.)						
7.7.4	Er det etablert et system eller prosedyre for rapportering av brudd på sikkerhetsbestemmelsene til driftskontrollsystemet?						
7.7.5	Er det gjennom disse prosedyrene en ordning som sørger for at rapportering om hendelser, svakheter, feil etc blir fulgt opp og ansvarliggjort?						
7.7.6	Har dere definert når, og laget en prosedyre for, rapportering til NVE ved en hendelse i driftskontrollsystemet?						
§ 7-8 Beredskap ved svikt i driftskontrollsystemet							
7.8.1	Er det planer for, eller på andre måter forberedt tiltak for fortsatt drift av anleggene dersom driftskontrollsystemet svikter?						
§ 7-9 Bemanning av driftssentral							
7.9.1	Har dere kompetente personer som til enhver tid kan bemanne driftssentralen og koble i nettet?						
7.9.2	Gjelder dette også i helgene, ved helligdager og ferier samt ved sykdom?						
7.9.3	Har dere evne til å påkalle ekstra bemanning til driftssentralen ved behov – også ved hendelser som varer flere dager?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
§ 7-10 Ekstern tilkobling til driftskontrollsystem							
7.10.4	Har dere utarbeidet en egen risikovurdering knyttet til bruk av ekstern tilkobling (fjernaksess) til driftskontrollsystemet?						
7.10.5	Er ordningen for fjernaksess (metode og sikringstiltak) gjennomgått og godkjent av virksomhetens ledelse eller ansvarlig person/seksjon/avdeling?						
7.10.6	Er det etablert en ordning (prosedyre, rutiner etc) for å godkjenne personell som har anledning til å koble seg på driftskontrollsystemet via fjerntilgang (gjelder både eget personell og eksterne leverandører/-samarbeidspartnere)						
7.10.7	Foreligger det en oppdatert liste over alle personer som er gitt tilgang til å kunne koble seg på driftskontrollsystemet via fjerntilgang?						
§ 7-11 Systemredundans i driftskontrollsystemet							
7.11.1	Er det foretatt en vurdering hvorvidt det er behov for systemredundans i driftskontrollsystemet?						
7.11.2	Er vurderingen dokumentert?						
<i>Kun for fjernvarmeselskap</i>							
7.11.3	Er det et annet selskap – og som ikke er KBO-enhet som utøver styring, regulering og overvåking (SRO) av fjernvarmesentralene og med tilhørende infrastruktur?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.11.4	Har dere påsett at virksomheten som ikke er KBO-enhet har beskyttet SRO-anlegget slik at relevante krav i beredskapsforskriften ivaretas?						
7.11.5	Kan dette dokumenteres?						
§ 7-12 Sammenkobling mellom avanserte måle- og styringssystem (AMS) og driftskontrollsystem							
7.12.1	Benytter KBO-enheten på noen områder felles infrastruktur for innhenting av måledata hos sluttkunder og toveiskommunikasjon med deres målerne (AMS), og driftskontrollsystemet som benyttes til overvåking og styring av virksomhetens anlegg?						
7.12.2	Er dette risikovurdert?						
7.12.3	For de delene som ovennevnte er sammenfallende, beskyttes både AMS-løsningen og driftskontrollsystemet på samme måte (systemsikkerhet, fysisk sikring etc)?						
§ 7-13 Beskyttelse mot elektromagnetisk puls og interferens							
7.13.1	Har virksomheten foretatt en vurdering hvorvidt det er behov for å sikre komponenter i driftskontrollsystemet mot elektromagnetisk puls og interferens?						
	Er dette dokumentert?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
§ 7-14 Særskilte krav til driftskontrollsystem i klasse 2							
<i>§ 7-14 a) Sikkerhetskopier</i>							
7.14.a1	Testes det jevnlig at gjenoppretting av sikkerhetskopier fungerer etter hensikten?						
7.14.a2	Er det utarbeidet rutiner/prosedyrer for hvor ofte dette skal skje, og hvordan det skal skje?						
<i>§ 7-14 b) Sikkerhetsrevisjon</i>							
7.14.b1	Er det gjennomført intern sikkerhetsrevisjon av driftskontrollsystemet siste året?						
7.14.b2	Er det etablert rutiner eller planer for jevnlig sikkerhetsrevisjon på driftskontrollsystemet?						
<i>§ 7-14 c) Overvåking og logging</i>							
7.14.c1	Er det etablert et system for overvåking og logging av unormal datatrafikk inn eller ut av driftskontrollsystemet?						
7.14.c2	Er det etablert en prosedyre/retningslinjer etc for hvordan virksomheten skal agere dersom dere får varsel om unormal trafikk?						
<i>§ 7-14 d) Utilgjengelig driftssentral</i>							
7.14.d1	Er det mulig å styre anleggene til virksomheten selv om det ikke er mulig å oppholde seg i driftssentralen?						
7.14.d2	Er det laget planer for alternativ drift av anleggene dersom det ikke er mulig å benytte driftssentralen over lengre tid (for eksempel i over én uke?)						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
§ 7-14 e) Bemanning av driftssentral							
7.14.e1	Er det etablert en ordning der alarmer fra driftskontrollsystemet umiddelbart blir mottatt og vurdert av kompetent personell – uansett tidspunkt?						
7.14.e2	Er det gjennomført en vurdering om hvilke hendelser/alarmer som krever at driftssentralen bemannes?						
7.14.e3	Er det mulig for alle operatører som inngår i vaktordningen å reise til og bemanne driftssentralen innen én time etter at første alarm/varsel om hendelse er mottatt?						
7.14.e4	Er det etablert en ordning der ekstra operatører kan tilkalles for å bemanne driftssentralen ved behov?						
7.14.e5	Er det gjort en vurdering av hvor terskelen går for å tilkalle ekstra personell?						
§ 7-14 f) Ekstern tilkobling til driftskontrollsystemet							
7.14.f1	Er det etablert en prosedyre/rutine som sikrer at driftssentralen er bemannet dersom leverandører skal kunne koble seg på driftskontrollsystemet via ekstern tilgang?						
7.14.f2	Er prosedyren/rutinen for ekstern tilkobling skriftlig – også i de tilfellene KBO-enheten egne medarbeidere skal koble seg på driftskontrollsystemet via ekstern tilkobling?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.14.f3	Er det etablert en prosedyre/rutine/tilgangskontroll etc som sikrer en positiv identifisering og autentisering av personen(e) som skal koble seg på driftskontrollsystemet via ekstern tilgang?						
7.14.f4	Har det blitt utarbeidet retningslinjer for hva KBO-enheten anser som «sikkert sted» for å kunne koble seg på driftskontrollsystemet ved hjelp av ekstern tilkobling?						
7.14.f5	Er det etablert en rutine/prosedyre som sørger for at den eksterne tilkoblingen til driftskontrollsystemet lukkes når den ikke lenger skal brukes?						
7.14.f6	Er det utarbeidet retningslinjer for når man kan koble i nettet (dersom det er mulig) når operatøren er påkoblet driftskontrollsystemet via ekstern tilkobling?						
7.14.f7	Er det utarbeidet en logg/register eller liknende der all tilkobling til driftskontrollsystemet via ekstern tilkobling registreres?						
§ 7-14 g) Systemredundans							
7.14.g1	Hvis det oppstår svikt i offentlige (kommersielle teletilbyderes) nett, vil sambandet i driftskontrollsystemet til anlegg i klasse 2 og 3 fremdeles fungere?						
7.14.g2	Er det redundant samband til alle anlegg i klasse 2 og 3 – helt inn til der det lokale kontrollanlegget begynner?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.14.g3	Er det fysisk separering i de redundante sambandsveiene på en slik måte at fysisk brudd i én sambandsvei ikke medfører at alle redundante sambandsveier faller ut samtidig?						
7.14.g4	Er det etablert vaktordninger med eget personell eller avtaler med eksterne leverandører som sikrer at reparasjonsarbeid ved brudd i sambandet starter så raskt som praktisk mulig? ¹						
7.14.g5	Er det avtalefestet responstid for oppstart av reparasjonsarbeid (utreise, feilfinning, feilretting etc)						
§ 7-14 h) Særskilt om dublering							
7.14.h1	Er det utarbeidet prosedyrer/retningslinjer eller liknende for å forebygge muligheten for at samme systemfeil rammer alle dublerne system samtidig? (for eksempel ved oppdatering, vedlikehold etc).						
§ 7-14 i) Beskyttelse mot EMP og EMI							
7.14.i1	Er det utført sikringstiltak eller beredskapstiltak for å beskytte utrustning i sambandsveiene til alle anleggene i klasse 2 og 3, og som blir styrt gjennom driftskontrollsystemet?						
§ 7-14 j) Sikker tidsreferanse							
7.14.j1	Er KBO-enheten avhengig av sikker tidsangivelse?						

¹ Her må man selvfølgelig ta hensyn til om det er sikkert å dra inn i områdene der sambandsbruddet har oppstått – for eksempel etter et uvær.



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
7.14.j2	Hvis ja, har enheten sørget for at tidsangivelsen kommer fra sikre kilder?						
§ 7-15 Særskilte krav til driftskontrollsystem i klasse 3							
<i>§ 7-15 a) Reserve driftssentral</i>							
7.15.a1	Har enheten etablert en reserve driftssentral på annen fysisk lokasjon enn den ordinære driftssentralen?						
7.15.a2	Har enheten forsikret seg om at reserve driftssentral til enhver tid er klar til bruk?						
7.15.a3	Er reserve driftssentral utstyrt på en slik måte at man i reserve driftssentral kan overta overvåking og styringen av alle anleggene som driftskontrollsystemet styrer?						
7.15.a4	Kan overvåking og styring av reserve driftssentral foregå helt uavhengig av ordinær driftssentral?						
7.15.a5	Har reserve driftssentral et fysisk sikringsnivå som kreves for klassen til driftskontrollsystemet for øvrig?						
<i>§ 7-15 b) Bemanning av driftssentral</i>							
7.15.b1	Er driftssentralen til enhver tid bemannet av kompetent personell?						
7.15.b2	Har enheten en ordning for påkalling av ekstra operatører som kan bemanne driftssentralen innen én time etter at påkalling er gjort?						
7.15.b3	Er det etablert en fast rutine der enheten minst årlig evaluerer driftssentralens bemanning?						
7.15.b4	Er evalueringen dokumentert?						



Nr	Kontrollspørsmål	Ja	Nei	Hvis nei, hvorfor?	Tiltak	Tidsfrist	Ansvarlig
§ 7-15 c) Ekstern tilkobling til driftskontrollsystem							
7.15.c1	Har enheten etablert tekniske og/eller systemmessige tiltak som gjør at det ikke er mulig å utføre kobling eller styring av anlegg via ekstern tilgang til driftskontrollsystemet?						
§ 7-15 d) Systemredundans							
7.15.d1	Kan enheten dokumentere at sambandsveiene i driftskontrollsystemet til anlegg i klasse 3 er utført så sikre og robuste og med en slik redundans at man ved samtidige eller påfølgende hendelser ikke skader begge føringsveier eller andre redundante delsystem?						
7.15.d2	Har enheten full kontroll og råderett over alle komponenter eller tekniske løsninger i minst én sambandsvei til anlegg i klasse 3?						
§ 7-15 e) Beskyttelse mot EMP og EMI							
7.15.e1	Er minst én sambandsvei til anlegg i klasse 3 beskyttet mot EMP eller EMI?						
7.15.e2	Er det etablert EMP-beskyttelse eller beredskapstiltak for minst én sambandsvei til anlegg i klasse 2?						
§ 7-15 f) Fastsettelse av særlige krav til bemanning							
	Ingen spørsmål						
§ 7-16. Vern av kraftsystem i regional- og sentralnett							
	Ingen spørsmål						

Denne serien utgis av Norges vassdrags- og energidirektorat (NVE)

Utgitt i Veilederserien i 2013

Nr. 1 Veiledning til forskrift om forebyggende sikkerhet og beredskap i energiforsyningen



Norges
vassdrags- og
energidirektorat

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 09575
Internett: www.nve.no