Foreløpig tilleggsveileder til kraftberedskapsforskriften

Oppdateringer etter revisjon

Norges vassdrags- og energidirektorat
2018

Innhold

1 Innledning

Hensikten med forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften) er å stille krav som sikrer at kraftforsyningen opprettholdes og at normalt forsyning gjenopprettes på en sikker og effektiv måte i og etter ekstraordinære situasjoner.

Den digitale utviklingen både i energisektoren og samfunnet for øvrig medfører en endring i kraftsystemets risiko- og sårbarhetsbilde. Dette søker endringsforskriften å møte med blant annet nye bestemmelser om IKT-sikkerhet.

Dette dokumentet er en foreløpig tilleggsveileder til NVE veileder 1/2013. Tilleggsveilederen omtaler kun nye bestemmelser og andre endringer av innholdsmessig betydning. Rent språklige endringer og omstruktureringer er i utgangspunktet derfor ikke omtalt.

NVE veileder 1/2013 gjelder fremdeles, så langt ikke annet følger av tilleggsveilederen. NVE viser til vedlegg 1 for en oversikt. Av vedlegg 2 følger en oversikt over hvilke bestemmelser som gjelder/kan gjelde for hvem jf. § 1-3.

Vi tar sikte på å revidere hele veilederen i løpet av 2019.

NVE viser til NVE rapport nr. 92/2018 Oppsummeringsdokument: Endringer i beredskapsforskriften – Krav til IKT-sikkerhet m.m. og NVE høringsdokument 6:2017 for utfyllende informasjon om forskriftsendringene.

2 Endringer i kapittel 1

§ 1-3. Hvem forskriften gjelder for

§ 1-3. ***Hvem forskriften gjelder for***

Forskriften gjelder for de virksomheter som er KBO-enheter etter § 2-1 annet ledd bokstav a eller som er blitt KBO-enheter etter § 2-1 annet ledd bokstav b. For KBO-enheter gjelder bestemmelsene rettet til KBO-enheter og virksomheter.

Beredskapsmyndigheten kan ved enkeltvedtak bestemme at deler av forskriften skal gjelde for andre virksomheter som helt eller delvis eier eller driver anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme. For virksomheter som ikke er KBO-enheter, er det kun de bestemmelser som er rettet til virksomheter som kan gis anvendelse.

Beredskapsmyndigheten kan ved enkeltvedtak bestemme at §§ 6-3 og 6-4 skal gjelde for andre virksomheter enn de som er omfattet av første eller annet ledd.

Forskriften § 6-2 om taushetsplikt for kraftsensitiv informasjon gjelder for enhver.

Hvorfor vi har bestemmelsen

NVE mener det er viktig å klargjøre både hvem forskriften gjelder for og hvilke krav som gjelder for hvem. Andre virksomheter enn KBO-enheter er derfor ikke omfattet av forskriften uten at beredskapsmyndigheten har fattet vedtak om dette (med unntak av § 6-2 som gjelder enhver). Vi viser til punkt 1.2 i oppsummeringsdokumenter for bakgrunn og kommentarer til endringen.

Hvilke krav gjelder for hvem

Se vedlegg 2.

Ordforklaringer

Ord	**Forklaring**
Anlegg	*Fysiske anlegg som kraftstasjon, transformatorstasjon og fjernvarmeanlegg med de komponenter og bygningsdeler som inngår i disse.*
System	*Driftskontrollsystemer og andre IKT-systemer*
Annet	*Andre bygninger eller komponenter som har betydning, som for eksempel lagerbygg som inneholder beredskapsmateriell.*

3 Endringer i kapittel 2

§ 2-2. Organisasjon og funksjon

§ 2-2. ***Organisasjon og funksjon***

KBO-enheter skal ha følgende funksjoner, som utpekes av leder for virksomheten:
a. *Beredskapsleder.* Denne skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet.

b. *Beredskapskoordinator.* Denne skal ha oversikt over beredskapsarbeidet i virksomheten og være administrativt kontaktpunkt til beredskapsmyndigheten.

c. *IKT-sikkerhetskoordinator.* Denne skal ha oversikt over IKT-sikkerhetsarbeidet i virksomheten og være faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet.

Hvorfor vi har bestemmelsen

Formålet er å sikre at det blir utpekt personer i virksomhetene som skal ha et særlig ansvar for at kravene i kraftberedskapsforskriften etterleves.

Videre er formålet med utpeking av disse rollene at KBO-enheten utvikler nødvendig kompetanse til å sikre anlegg og systemer, ha beredskap for å håndtere ekstraordinære situasjoner.

Hvem bestemmelsen gjelder for

KBO-enheter.

Hvordan kravene kan oppfylles

Det er her ført inn nye krav til beredskapskoordinator og IKT-sikkerhetskoordinator. Kravene fremgår tydelig av forskriftsteksten, og kommer i tillegg til det som er beskrevet i tidligere veileder. Funksjonene til beredskapsleder er beskrevet i NVE veileder 1/2013.

§ 2-5. Varsling

§ 2-5. ***Varsling***

KBO-enheter skal uten ugrunnet opphold varsle beredskapsmyndigheten om ekstraordinære situasjoner. Situasjoner som angitt i § 2-6 bokstav a til h om rapportering, skal alltid varsles. Varselet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson.

Hvorfor vi har bestemmelsen

Formålet er å sikre at NVE raskt får relevant informasjon om ekstraordinære situasjoner som kan ha betydning for forsyningssikkerheten. NVE kan få flere varsler som, spesielt i en tidlig fase, til sammen viser at situasjonen er mer alvorlig enn først antatt for det enkelte selskap.

Hvem bestemmelsen gjelder for

KBO-enheter.

Ordforklaringer

Ord	Forklaring
Uten ugrunnet opphold	*Uten ugrunnet opphold betyr så snart som praktisk mulig. Uten ugrunnet opphold innebærer at den som er ansvarlig ikke kan utsette eller nedprioritere oppgaven uten at det foreligger en begrunnelse som kan forsvare dette. Vi presiserer at det første varselet til NVE er ment å være kort.*

Hvordan kravene kan oppfylles

NVE har valgt å tydeliggjøre forskjellen mellom varsling og rapportering ved å dele dette inn i to separate paragrafer. Det er også tydeliggjort at hendelsene som er nevnt i §2-6 skal varsles i tillegg til å rapporteres i etterkant.

Maler for varsling og rapportering er tatt ut av veilederen, men skal fortsatt ligge i forenklet versjon på NVEs nettsider.

Listen i §2-6 bokstav a-h angir hendelser som kan forårsake en ekstraordinær situasjon, men listen er ikke uttømmende. KBO-enheten må selv vurdere om det er andre situasjoner som beredskapsmyndigheten bør være kjent med. Et eksempel på en situasjon som i tillegg bør varsles, er når forsyningssikkerheten er dårligere på grunn av N-0 drift. Et annet eksempel er at det er stor medieoppmerksomhet rundt en situasjon. Det kan være varslingspliktig selv om det ikke i seg selv gir en rapporteringsplikt etter § 2-6.

Av forskriftsteksten følger at NVE skal motta varsel om alle situasjoner som angitt i § 2-6 bokstav a-h. NVE vil etter hvert delegere oppgaver i forbindelse med varsling av IKT-sikkerhetshendelser til KraftCERT. Ekstraordinære IKT-sikkerhetshendelser skal likevel fremdeles varsles til NVE. Varsling av IKT-hendelser er også kort omtalt i veileder til § 6-9. Informasjon til fylkesmenn og kommuner er omtalt i § 2-8.

Det er ingen formkrav til hvordan varselet skal se ut, men forskriftsteksten stiller enkle krav til innhold. På NVEs nettsider ligger i tillegg en oversikt over hvilken informasjon det er relevant å oppgi i et varsel.

Dersom man er i tvil om en situasjon skal varsles, bør man varsle NVE.

§ 2-6. Rapportering

§ 2-6. ***Rapportering***

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. Ved begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten eller andre virksomheter.

d. Situasjoner hvor kraftsensitiv informasjon 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 transmisjon- 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 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 annet ledd.

Hvorfor vi har bestemmelsen

Formålet er å sikre at NVE får god oversikt over hendelser som har eller kunne ha påvirket forsyningssikkerheten. Det er ikke en forutsetning at situasjonen faktisk har ført til avbrudd i energiforsyningen.

NVE har valgt å tydeliggjøre forskjellen mellom varsling og rapportering ved å dele dette inn i to separate bestemmelser.

Hvem bestemmelsen gjelder for

KBO-enheter.

Ordforklaringer

Ord	**Forklaring**
Begrunnet mistanke	*I begrepet begrunnet mistanke ligger et krav om at det må være en viss grad av sannsynlighet for at en hendelse vil inntreffe. Mistenkelig adferd kan gi begrunnet mistanke- Også andre omstendigheter, eksempelvis funn av gjenstander eller en observert unormal tilstandsendring i et system, kan ligge til grunn for at man har en begrunnet mistanke.*

Viktige samfunnsfunksjoner	*Viktige samfunnsfunksjoner omfatter mer enn kritiske samfunnsfunksjoner. Kritiske samfunnsfunksjoner vil alltid være viktige samfunnsfunksjoner.* *Kritisk samfunnsfunksjon er knyttet opp mot samfunnets grunnleggende behov som er definert som trygghet for den enkelte og basale fysiske behov som vann, mat, varme og lignende. Kritiske samfunnsfunksjoner inkluderer vannforsyning, varmeforsyning, matvareforsyning, finansiell trygghet, nasjonal sikkerhet, lov og orden, liv og helse, kriseledelse.*[1]

Hvordan kravene kan oppfylles

En rapport skal inneholde mer informasjon enn et varsel. På NVEs nettsider ligger det to maler som skal brukes til rapportering av ulike typer hendelser.

I noen tilfeller har NVE behov for mer informasjon enn det som fremgår av malen. I slike tilfeller vil NVE be om utfyllende skriftlig informasjon som kommer i tillegg til den ordinære rapporteringsmalen. KBO-enheten kan også uoppfordret rapportere om forhold som de mener beredskapsmyndigheten bør gjøres oppmerksom på.

Bokstav a-h er forhold som *skal* rapporteres. Virksomheten må selv vurdere om det er andre ekstraordinære situasjoner som *bør* rapporteres til beredskapsmyndigheten. Eksempel er situasjoner som ikke førte til utfall, men som kunne fått konsekvenser for forsyningssikkerheten.

Dersom man er i tvil om en situasjon skal rapporteres, kan man ta kontakt med NVE for å avklare dette.

Maler for varsling og rapportering vil bli tatt ut av veileder 1/2013 1.1.2019, men vil fortsatt ligge i forenklet versjon på NVEs nettsider.

[1] Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring, KIKS-prosjektet – 1. delrapport, DSB 2012, s 15-16, https://www.dsb.no/globalassets/dokumenter/rapporter/sikkerhet-i-kritisk-infrastruktur.pdf

4 Endringer i kapittel 3

§ 3-6. Sektorvist responsmiljø

§ 3-6. ***Sektorvist responsmiljø for IKT-sikkerhetshendelser***

Beredskapsmyndigheten er sektorvist responsmiljø for IKT-sikkerhetshendelser i kraftforsyningen.

Beredskapsmyndigheten kan delegere oppgaver innenfor varsling, informasjonsdeling og analyse for IKT-sikkerhetshendelser i kraftforsyningen til en eller flere KBO-enheter.

Hvorfor vi har bestemmelsen

Formålet er for det første å gjøre det tydelig at det er NVE som beredskapsmyndighet som er sektorvist responsmiljø. For det andre er formålet å gjøre det forutsigbart hvilke oppgaver NVE kan delegere til hvem.

NVE er en del av det nasjonale systemet for hendelseshåndtering og beredskap.

NVE viser til nasjonale beredskapsplaner og til «Rammeverk for håndtering av IKT-sikkerhetshendelser».[2] [3]

IKT-sikkerhetshendelser som faller inn under rammeverkets virkeområde skal håndteres gjennom en systematisk prosess bestående av 1) planlegging og forberedelse; 2) deteksjon og vurdering av omfang og alvorlighetsgrad; 3) varsling av relevante parter; 4) iverksetting av prosesser og tiltak for å håndtere hendelsen; 5) situasjonsrapportering og 6) tilbakeføring og læring av hendelsen. Prosessen er gjennomgående for de tre nivåene som rammeverket bygger på: a) virksomheter/systemeiere, b) sektorvise responsmiljøer (SRM) med fullmakt fra departement og c) NSM på nasjonalt sektorovergripende nivå.

Den enkelte virksomhet som forvalter kritisk infrastruktur og/eller kritiske samfunnsfunksjoner skal utøve sin rolle og sitt ansvar raskt og formålseffektivt som del av en større, koordinert respons for å gjenopprette sikker tilstand for berørte systemer, utføre skadevurdering og begrense følgeskader for andre IKT-systemer.

Hvem bestemmelsen gjelder for

Beredskapsmyndighet for kraftforsyning.

[2] Rammeverk for håndtering av IKT-sikkerhetshendelser, Versjon per 07.12.17, https://nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

[3] Rammeverk for håndtering av IKT-sikkerhetshendelser, https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

Ordforklaringer

Ord	Forklaring
Sektorvist responsmiljø	*En utpekt funksjon innen en samfunnssektor eller overordnet styringsområde, med grunnleggende kapasitet til å koordinere og håndtere uønskede IKT-sikkerhetshendelser.*

5 Endringer i kapittel 5

§ 5-2. Klasser

§ 5-2. *Klasser*

Ved klassifisering av anlegg, system 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 kraftforsyningen er størst.

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

Vindkraftanlegg klassifiseres ikke som kraftstasjon.

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

Denne bestemmelse omfatter ikke midlertidige anlegg eller midlertidige løsninger som del av anlegg 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 50 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. Transformatorstasjon til vindkraftanlegg med samlet installert ytelse på minst 75 MVA. Dersom transformatorstasjonen også transformerer til nettformål, klassifiseres den som transformatorstasjon etter bokstav b.
h. Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til g.

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. Transformatorstasjon til vindkraftanlegg med samlet installert ytelse på minst 500 MVA. Dersom transformatorstasjonen også transformerer til nettformål, klassifiseres den som transformatorstasjon etter bokstav b, men ikke lavere enn klasse 2.
h. Driftskontrollsystem som styrer eller overvåker kraftforsyningen til befolkning på minst 50 000, eller flere anlegg omfattet av bokstav a til g.

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 som styrer eller overvåker kraftforsyningen til befolkning på minst 250 000, eller flere anlegg omfattet av bokstav a til d.

Hvorfor vi har bestemmelsen

Formålet er å skille mellom ulike anlegg, system eller annet på en systematisk måte etter hvor stor betydning det har for drift eller gjenoppretting av produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme. Klasse 3 benyttes der betydningen for kraftforsyningen er størst.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3.

Ordforklaringer

Ord	**Forklaring**
Installert generatorytelse	*Summen av merkeytelsen (på merkeskilt) for hver generator i kraftstasjonen*
Hovedtransformatorytelse	*Ytelsen til de transformatorer som ivaretar anleggets primære transformeringsformål. Ved redundans i anlegget regnes summen av ytelsen for alle de aktuelle krafttransformatorene. Det er nominell ytelse som angitt på merkeskilt som gjelder.*
Selvstendig koblingsstasjon	*Koblingsanlegg som funksjonelt ikke tilhører en kraft- eller transformatorstasjon, eller som har en viktigere funksjon enn stasjonen det er tilknyttet. Som koblingsstasjon regnes som regel et fullverdig anlegg med samleskinne, brytere og felt for flere avganger for kraftledninger.*

Hvordan kravene kan oppfylles

I forskriften er det en opplisting av hvilke anlegg, system eller annet som inngår i hver klasse. For å gi en bedre oversikt over hvilken klasse ulike typer anlegg havner i, gir vi nedenfor en oversikt basert på anleggstype.

NVE kan treffe vedtak om at anlegg, system eller annet skal klassifiseres i en annen klasse enn det som følger av § 5-2 dersom det anses nødvendig jf. § 5-7 annet ledd.

Kraftstasjoner (bokstav a)

- Klasse 1 - Kraftstasjon med samlet installert generatorytelse på minst 50 MVA
- Klasse 2 - Kraftstasjon med samlet installert generatorytelse på minst 100 MVA
- Klasse 3 - Kraftstasjon i fjell med samlet generatorytelse på minst 250 MVA

Transformatorstasjoner og vindkraft (bokstav b og g)

Hvis transformatorstasjonen har transformering for nettformål, er det kriteriene for ytelse for transformatorstasjon etter bokstav b for klasse 2 og 3 som gjelder. Dette gjelder likevel ikke dersom transformering til vindkraftanlegget har så stor ytelse at den kommer i en høyere klasse.

- Klasse 1 - Transformatorstasjon med samlet hovedtransformatorytelse på minst 10 MVA. Transformatorstasjoner som kun er tilknyttet vindkraftanlegg inngår kun i klasse 1 om ytelsen er større enn 75 MVA.

- Klasse 2 - Transformatorstasjon med samlet ytelse for omforming på minst 50 MVA og høyeste spenningsnivå på minst 30 kV. Transformatorstasjoner som kun er tilknyttet vindkraftanlegg inngår i klasse 2 om ytelsen er større enn 500 MVA.
- Klasse 3 - Transformatorstasjon med samlet ytelse for omforming på minst 100 MVA og bygget for et høyeste spenningsnivå på minst 200 kV og transformering til sekundært spenningsnivå i nett på minst 30 kV.

Omformerstasjon (bokstav c, klasse 1 og 2)

- Klasse 1 - Omformerstasjon med samlet ytelse for omforming på minst 10 MVA.
- Klasse 2 - Omformerstasjon med samlet ytelse for omforming på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.

Selvstendig koblingsstasjon (bokstav d klasse 1 og 2, bokstav c klasse 3)

- Klasse 1 - Selvstendig koblingsstasjon bygget for et spenningsnivå på minst 30 kV.
- Klasse 2 - Selvstendig koblingsstasjon bygget for et spenningsnivå på minst 100 kV.
- Klasse 3 - Selvstendig koblingsstasjon bygget for et spenningsnivå på minst 200 kV.

Kraftledning (bokstav e klasse 1 og 2, bokstav d klasse 3)

- Klasse 1 - Kraftledning bygget for et spenningsnivå på minst 5 kV.
- Klasse 2 - Kraftledning bygget for et spenningsnivå på minst 30 kV.
- Klasse 3 - Kraftledning bygget for et spenningsnivå på minst 200 kV.

Fjernvarmesentral (bokstav f klasse 1 og 2)

Grensen gjelder installert ytelse i selve fjernvarmesentralen og inkluderer også eksternt tilført energi fra for eksempel søppelforbrenningsanlegg og varmepumper.

- Klasse 1 - samlet installert ytelse på minst 50 MW.
- Klasse 2 - samlet installert ytelse på minst 150 MW.

Driftskontrollsystem

Driftskontrollsystemets klasse bestemmes enten av den høyeste klassen på de anleggene den styrer, eller ut fra befolkningstall for de kommunene driftssentralen overvåker kraftforsyningen til. Det er befolkningstall fra Statistikks sentralbyrå (SSB)[4] som skal legges til grunn for befolkningstallet. SSB utgir årlige statistikker på befolkningstall. Selv om forsyningsområdet er delt på tvers av kommuner, kan det tas utgangspunkt i befolkningen for hele kommunen. Befolkningstall skal ikke legges til grunn for driftkontrollsystemer som kun styrer og overvåker kraftproduksjon.

Regionalnettseiere regner befolkning i eget konsesjonsområde pluss området til øvrige områdekonsesjonærer som mates fra deres regionalnett. Om befolkningstallet ligger tett opp mot grensen, anbefaler NVE at selskapet velger den høyeste klassen for sikringstiltakene. NVE minner om at det alltid skal ligge en risikovurdering til grunn for sikringstiltakene jf. § 2-3. Følgende grenser gjelder:

[4] https://www.ssb.no/befolkning/statistikker/folkemengde/aar-per-1-januar
https://www.ssb.no/befolkning/statistikker/folkemengde/aar-per-1-januar#relatert-tabell-1

- Klasse 1: Driftkontrollsystem som styrer eller overvåker anlegg i klasse 1
- Klasse 2: Driftkontrollsystem som styrer eller overvåker flere anlegg i klasse 2, eller som styrer eller overvåker kraftforsyningen til en befolkning på mellom 50 000 og 250 000.
- Klasse 3: Driftkontrollsystem som styrer eller overvåker flere anlegg i klasse 3, eller som styrer eller overvåker kraftforsyningen til en befolkning på minst 250 000.

§ 5-9. Meldeplikt om sikringstiltak

> **§ 5-9.** ***Meldeplikt om sikringstiltak***
>
> Virksomheter som planlegger å bygge, endre eller utvide anlegg, system eller annet, skal i god tid før arbeidets oppstart sende beredskapsmyndigheten skriftlig melding om hvilken klasse det vil bli utført etter, jf. § 5-2. Meldingen skal bekrefte at arbeidet vil skje i samsvar med kravene i §§ 5-4 til 5-6.
>
> Melding skal gis på den måten beredskapsmyndigheten bestemmer. Meldingen skal være vedlagt den informasjon som beredskapsmyndigheten bestemmer.

Hvorfor vi har bestemmelsen

Formålet er å sikre at anlegget, systemet eller annet er riktig klassifisert og godt nok sikret i henhold til sin klasse. Sikringstiltak må planlegges og prosjekteres tidlig i prosessen, slik at sikringstiltakene kan utføres på en mest mulig hensiktsmessig måte og kostnadene reduseres. NVE bruker også meldingen for å holde oppdatert oversikt over klassifiserte anlegg.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3.

Hvordan kravene kan oppfylles

Alle anlegg som skal klassifiseres etter § 5-2 er meldepliktige. NVE har skjema for «Melding om sikring av konsesjonspliktige anlegg»[5] på https://www.nve.no/media/2308/vedlegg-1-melding-sikring-konsjonspliktig-anlegg.pdf. Dette skal også benyttes for alle meldepliktige anlegg, ikke kun konsesjonspliktige anlegg. Dette gjelder altså anlegg, system eller annet som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme.

Meldingen må sendes i så god tid at det er mulig for virksomheten å forholde seg til eventuelle krav fra NVE. Det er opp til virksomheten selv å vurdere hva som er tilstrekkelig tid. Det må regnes med saksbehandlingstid i NVE. Hva som er god tid, kommer blant annet an på omfanget av hva som bygges, endres og utvides, samt hvilke krav til sikringstiltak som gjelder. NVE ser det derfor ikke hensiktsmessig å angi en bestemt frist for når melding skal sendes. Tidligere har det vært krav om å sende melding

[5] https://www.nve.no/media/2308/vedlegg-1-melding-sikring-konsjonspliktig-anlegg.pdf

i forbindelse med konsesjonssøknad for konsesjonspliktige anlegg. God tid må forstås som minst tre til seks måneder før oppstart av arbeidet.

§ 5-11. Restriksjoner for adgang til steder og områder

§ 5-11. ***Restriksjoner for adgang til steder og områder***

Alle driftssentraler i klassifiserte driftskontrollsystemer, og alle anlegg klassifisert i klasse 3, skal ha restriksjoner for adgang. Beredskapsmyndigheten kan vedta at også anlegg i klasse 2 skal ha restriksjoner for adgang.

Ved anlegg underlagt restriksjoner for adgang 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. Fotografering være forbudt med mindre spesiell tillatelse er innhentet fra ansvarlig representant for anlegget.

For driftssentraler i driftskontrollsystemer i klasse 3 er det forbudt med besøkende og fotografering. Personer uten full bakgrunnssjekk etter § 6-7 skal ikke ha adgang til driftssentraler i klasse 3. Beredskapsmyndigheten kan vedta det samme for andre anlegg i klasse 3

Hvorfor vi har bestemmelsen

Formålet er å forebygge og forhindre uønsket informasjonsinnhenting, plassering av uvedkommende gjenstander, sabotasje, trusler og vold mot ledelse og personell, eller urettmessig inngripen eller overtakelse.

I ny sikkerhetslov er det hjemmel til å nekte personer adgang til steder og områder i §7-5. Sikkerhetsloven benytter begrepet «nekte adgang», mens tidligere bfe. §5-11 brukte begrepet «besøksrestriksjoner». Bestemmelsen er endret slik at det kommer klarere frem at vi ønsker å sette restriksjoner på enhver type adgang, uavhengig av om man er ansatt i virksomheten eller er ekstern besøkende.

NVE vurderer det likevel som beskrivende å omtale personer som besøker anlegg som er underlagt restriksjoner som «besøkende» i opplistingen i annet og tredje ledd. Med besøkende menes for eksempel turister, skoleklasse, foreninger, medier og andre som ikke har tjenstlig behov for adgang.

I tredje ledd er det satt strengere krav til adgang til driftssentraler i klasse 3. Adgang til driftssentraler i driftskontrollsystemer i klasse 3 gir tilgang til spesielt sensitiv informasjon om kraftforsyningen og tilgang til system hvor sabotasje vil gi stor negativ konsekvens for kraftforsyningen. Den sensitive informasjonen gjelder ikke bare det som direkte vises av informasjon i driftssentralen, men også detaljer om beliggenhet, sikring, adgangskontroll m.m.

Anleggene i kraftforsyningen er klassifisert etter kritikalitet. Driftskontrollsystemer er de anleggene i kraftforsyningen der konsekvensene av sabotasje og innsideangrep er størst, og trusselnivået har økt siden forrige forskriftsrevisjon.

Hvem bestemmelsen gjelder for

KBO-enheter.

Ordforklaringer

Ord	**Forklaring**
Driftssentral	*Omfatter operatørrom, datamaskinrom, sambandsrom og andre rom som inneholder nødvendige komponenter for sentralens drift, inkludert tilhørende utstyr.*
Full bakgrunnssjekk	*Generell bakgrunnssjekk etter § 6-7 første ledd, samt innhenting av kredittsjekk etter annet ledd.*
Adgang	*Fysisk adgang. Logisk tilgang til systemer og annet er ikke omfattet av dette begrepet.*

Hvordan kravene kan oppfylles

De som er underlagt denne bestemmelsen skal ha rutiner for restriksjon for adgang i sitt internkontrollsystem.

Det er ikke tillatt å fotografere inne på driftssentraler i driftskontrollsystem i klasse 3. Når KBO-enheten selv har behov for å fotografere for dokumentasjon, kan dette gjøres så lenge fotoopptaket beskyttes som kraftsensitiv informasjon. Dette må fremgå av rutinene.

Videre er det ikke adgang til å tillate personer uten full bakgrunnssjekk adgang til driftssentraler i klasse 3. Dette må fremgå av virksomhetenes rutiner.

For driftssentraler i klasse 3 er full bakgrunnssjekk obligatorisk uavhengig av risikovurdering. Kravet i § 5-11 tredje ledd er i motsetning til § 6-7 ikke begrenset til egne ansatte. For utdypende forklaring om forholdet mellom § 5-11 og § 6-7, se oppsummeringsdokumentet.

6 Endringer i kapittel 6

§ 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere

§ 6-1. ***Identifisering av kraftsensitiv informasjon og rettmessige brukere***

KBO-enheter skal etter energiloven § 9-3 første ledd identifisere hva som er kraftsensitiv informasjon, hvor denne befinner seg og hvem som har tilgang til den.

Identifiseringen av hva som er kraftsensitiv 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 kraftsensitiv informasjon. Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for kraftsensitiv informasjon innenfor sin virksomhet.

Den enkelte KBO-enhet kan avgjøre om det er tjenstlig behov for å videreformidle kraftsensitiv informasjon til andre utenfor egen virksomhet. Den som har fått tilgang til kraftsensitiv informasjon av en KBO-enhet kan ikke videreformidle den kraftsensitive informasjonen til andre. Beredskapsmyndigheten kan i tvilstilfeller avgjøre hvem som er rettmessig bruker.

Hvorfor vi har bestemmelsen

Formålet er å tydeliggjøre hvilket ansvar KBO-enheten har for håndtering av kraftsensitiv informasjon.

Hvem bestemmelsen gjelder for

KBO-enheter. Fjerde ledd gjelder enhver som har fått tilgang til kraftsensitiv informasjon.

Ordforklaringer

Ord	**Forklaring**
Kraftsensitiv informasjon	*Se kbf. § 6-2 og enl. § 9-3.*
Tilgang	*Tilgang til fysiske dokumenter, digitalt lagret informasjon i form av filer og databaser, og vedlegg eller innhold (inkludert tale) i kommunikasjon.*
Enhver	*Fysisk og juridisk person*

Hvordan kravene kan oppfylles

Se foreløpig eksisterende veileder (NVE 2013).

§ 6-2. Kraftsensitiv informasjon

§ 6-2. ***Kraftsensitiv informasjon***

Kraftsensitiv informasjon er underlagt taushetsplikt etter § 9-3 i energiloven.

Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for kraftforsyningen, 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. Oversikt over rørnett for fjernvarme til samfunnsviktige funksjoner.
e. Nøyaktig kartfesting av jordkabler. Nøyaktig kartfesting av rørnett i fjernvarmeanlegg med varmesentraler i klasse 2.
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.

Hvorfor vi har bestemmelsen

Formålet er å tydeliggjøre hva slags informasjon som er kraftsensitiv.

Hvem bestemmelsen gjelder for

Enhver, herunder KBO-enheter og andre virksomheter med vedtak etter § 1-3.

Ordforklaringer

Ord	**Forklaring**
Driftskontrollfunksjoner	*Se kbf § 7-1. første ledd*

Hvordan kravene kan oppfylles

Se foreløpig eksisterende veileder (NVE 2013). Merk endringer som er gjort i bokstav § 6-2 annet ledd bokstav e om rørnett.

§ 6-3. Beskyttelse, avskjerming og tilgangskontroll

§ 6-3. ***Beskyttelse, avskjerming og tilgangskontroll***

Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv 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 kraftsensitiv informasjon.

Hvorfor vi har bestemmelsen

Formålet er å sikre at virksomheter som behandler kraftsensitiv informasjon sørger for å beskytte denne tilstrekkelig.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet eller tredje ledd.

Ordforklaringer

Ord	Forklaring
Mobile enheter	*Bærbare enheter for kommunikasjon og informasjonsbehandling, herunder bærbare datamaskiner, nettbrett, kameraer og mobil-telefoner med tilkoblet tilbehør. Også droner med video- og audioutstyr ombord vil kunne utgjøre en mobil enhet.*

Hvordan kravene kan oppfylles

Se foreløpig eksisterende veileder (NVE 2013).

For mobile enheter er i tillegg følgende råd viktige:

- Oppdater fastvare, operativsystem og applikasjoner (apper), og aktiver automatisk oppdatering der det er mulig
- Installer kun pålitelige applikasjoner (apper), kun fra pålitelige kilder.
- Installer programvare som sporer enheter når de blir borte, og sørger for fjernlåsing eller sletting ved tyveri og tap
- Ta sikkerhetskopi eller sørg for automatisk sikkerhetskopiering av viktig informasjon
- Etabler flåtestyring av mobile enheter som inkluderer påtvungen sikkerhetspolicy (for eksempel låseskjerm og kryptering), automatisk konfigurasjon og oppdatering av e-post og trådløst nett, og sletting av usikre applikasjoner (apper)
- Håndhev bestemmelser om forbudssoner for mobile enheter
- Bevisstgjør brukerne på hvilke bilder og hvilken informasjon som ikke bør lagres på mobile enheter

§ 6-4. Sikkerhetsinstruks

§ 6-4. ***Sikkerhetsinstruks***

Virksomheter som har eller behandler kraftsensitiv informasjon skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Sikkerhetsinstruksen skal beskrive 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 stille krav til undertegning av taushetserklæring. Sikkerhetsinstruksen skal også omfatte informasjon om at taushetsplikten medfører at kraftsensitiv informasjon ikke skal offentliggjøres.

Formål/bakgrunn

Formålet er å sikre at virksomheter som behandler kraftsensitiv informasjon sørger for å beskytte denne tilstrekkelig.

Hvem bestemmelsen retter seg mot

KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet eller tredje ledd.

Hvordan oppfylle kravene

Se foreløpig eksisterende veileder (NVE 2013).

Mal for taushetserklæring vil bli oppdatert.

§ 6-5. Anskaffelser

§ 6-5. ***Anskaffelser***

KBO-enheter har ansvaret for at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas i anskaffelser. KBO-enheter skal i anskaffelser påse at leverandører er forpliktet til å etterleve bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon.

Det skal i avtale sikres at KBO-enheter gis rett til å kontrollere, herunder revidere, leverandørens etterlevelse av disse bestemmelsene.

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.

Hvorfor vi har bestemmelsen

Formålet er å sikre at kravene til informasjonssikkerhet blir ivaretatt i alle ledd i en anskaffelsesprosess.

Hvem bestemmelsen gjelder for

Bestemmelsen gjelder for KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet ledd.

Hvordan kravene kan oppfylles

En måte å oppnå kravet på er at leverandøren legger fram tredjepartsrevisjonsrapport og at KBO-enheten får en gjennomgang av denne sammen med leverandøren. Se foreløpig eksisterende veileder (NVE 2013). Merk imidlertid at NVE er ikke lengre tilsynsmyndighet for leverandører. NVE kan likevel følge opp brudd på taushetsplikten i energiloven § 9-3 annet ledd som gjelder enhver.

§ 6-7. Personkontroll

§ 6-7. ***Personkontroll***

KBO-enheter skal gjennomføre en bakgrunnssjekk av personer før ansettelse.

KBO-enheter kan kreve at personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3 skal fremlegge kredittsjekk.

KBO-enheter skal før de fremsetter krav etter annet ledd foreta en risikovurdering. Kredittsjekk skal ikke anvendes dersom det kan iverksettes andre egnede sikkerhetstiltak.

Bakgrunnssjekken etter første og annet ledd skal brukes som grunnlag for å vurdere en persons egnethet til å få tilgang til klassifiserte anlegg, system eller annet. Kredittsjekk skal slettes når egnethetsvurderingen er gjennomført.

Krav om personkontroll etter første til fjerde ledd gjelder ikke personer som er sikkerhetsklarert og autorisert etter den til enhver tid gjeldende lov om nasjonal sikkerhet (sikkerhetsloven).

Beredskapsmyndigheten kan etter søknad gi unntak fra kravene i første til fjerde ledd i denne bestemmelsen. Beredskapsmyndigheten kan ved vedtak fastsette krav om bakgrunnssjekk etter første til fjerde ledd for bestemte anlegg, system og annet.

Hvorfor vi har bestemmelsen

Formålet er å bidra til å sikre klassifiserte anlegg mot innsiderisiko.

Hvem bestemmelsen retter seg mot

KBO-enheter.

Ordforklaringer

Ord	**Forklaring**
Bakgrunnssjekk	*Bakgrunnssjekk er prosessen med å innhente, sammenligne og dokumentere informasjon om en person, i den hensikt å bekrefte eller avkrefte det kandidaten selv opplyser. Bakgrunns-sjekk består av identitetskontroll, verifisering av utdanning og arbeidserfaring, søk i adresseregistre og andre åpne kilder, sjekk av næringsinteresser og eventuell kredittsjekk. Full bakgrunnssjekk vil si at alle ovennevnte elementer inngår, samt kredittsjekk..*
Egnethetsvurdering	*Helhetsvurdering av om en person er egnet for tilsetting eller tilgang, basert på funn fra bakgrunnssjekken.*

Kredittsjekk	*Kontroll og vurdering av kredittverdigheten og betalingsevnen for en person. Kredittsjekk er en tjeneste som selges av kredittopplysningsbyråer. Samme som kredittvurdering.*

Hvordan kravene kan oppfylles

KBO-enheter skal gjennomføre en bakgrunnssjekk av personer før ansettelse.

NVE viser til veilederen *Sikkerhet ved ansettelsesforhold, før, under og ved avvikling*, utgitt av Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd[6].

KBO-enheter kan kreve at personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3 skal fremlegge kredittsjekk.

NVE viser til Datatilsynets nettsider for nærmere informasjon om kredittsjekk.[7]

KBO-enheter skal før de fremsetter krav etter annet ledd foreta en risikovurdering. Kredittsjekk skal ikke anvendes dersom det kan iverksettes andre egnede sikkerhetstiltak.

Dersom KBO-enheten etter en risikovurdering finner det nødvendig med bruk av kredittsjekk, bør det opplyses om dette i stillingsutlysninger. For fysisk adgang til driftssentraler i klasse 3 gjelder et absolutt krav om full bakgrunnssjekk, jf. kbf § 5-11.

Bakgrunnssjekken etter første og annet ledd skal brukes som grunnlag for å vurdere en persons egnethet for tilgang til klassifiserte anlegg, system eller annet. Kredittsjekk skal slettes når egnethetsvurderingen er gjennomført.

Risikofaktorer som taler imot egnethet er usunne eller mangelfulle holdninger til sikkerhet, misnøye og ustabil adferd, kontakt med kriminelle enkeltpersoner eller miljøer, indikasjoner på rus- eller dopmisbruk, svak økonomi eller overdrevet forbruk i forhold til inntekt. Mangel på samtykke til kredittsjekk kan i seg selv være en relevant faktor. Holdninger og uavklarte forhold fra bakgrunnssjekken bør søkes avklart gjennom intervju med den aktuelle personen.

Personopplysninger som behandles i forbindelse med egnethetsvurderingen, skal slettes så fort formålet med innhentingen er oppfylt. Opplysninger fra kredittsjekk skal slettes når egnethetsvurderingen er gjennomført. Behandling av personopplysninger må gjøres i samsvar med personvernloven. NVE viser til Datatilsynet for veiledning.

Krav om personkontroll etter første til fjerde ledd gjelder ikke personer som er sikkerhetsklarert og autorisert etter den til enhver tid gjeldende lov om nasjonal sikkerhet (sikkerhetsloven).

[6] Sikkerhet ved ansettelsesforhold - før, under og ved avvikling, utgitt av Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd, mai 2017.
[7] Kredittvurdering, Datatilsynet.

I disse tilfellene gjelder et eget klareringsregime. For sivil sektor er Sivil klareringsmyndighet[8] (SKM) den sentrale sikkerhetsklareringsmyndigheten.

§ 6-9. Digitale informasjonssystemer

§ 6-9. *Digitale informasjonssystemer*

Virksomheter skal sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter det digitale informasjonssystemets type, oppbygging og funksjon.

Virksomheter skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer, herunder:

a. *Identifisere og dokumentere*
   Virksomheter skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.

b. *Risikovurdering*
   Virksomheter skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.

c. *Sikre og oppdage*
   Virksomheter skal sikre sine digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser. Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres. Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.

d. *Håndtere og gjenopprette*
   Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.

e. *Tjenesteutsetting*
   Virksomheter skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.

f. *Sikkerhetsrevisjon*
   Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.

Hvorfor vi har bestemmelsen

Formålet er å fastsette en generell plikt for virksomhetene til å sikre alle sine informasjons- og kommunikasjonssystemer, uavhengig om systemene benyttes for

[8] Sivil klareringsmyndighet.

driftskontroll eller lagring, behandling og formidling av kraftsensitiv informasjon. Plikten gjelder også tjenesteutsatte (utkontrakterte) systemer.

Bakgrunnen er økt risiko for vidtrekkende feil eller uautorisert inntrenging som følge av digitalisering og sammenkobling av systemer. Utviklingen innebærer stadig mer tilrettelegging for overvåking og styring av anlegg, og større avhengighet til leverandører for vedlikehold og feilretting. Nasjonale kraftsystemer og markeder integreres tettere på tvers av landegrensene. Et høyere generelt sikkerhetsnivå er dessuten egnet til å dempe den totale risikoen når kunnskap om samhandling mellom systemer svikter.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet ledd.

Ordforklaringer

Ord	**Forklaring**
Digitale informasjons-systemer	*Samlebetegnelse for informasjons- og kommunikasjonsteknologi som en virksomhet anvender til operasjonelle og administrative formål. Systemer for generering, samling, lagring, behandling, forvaltning og formidling av data og informasjon, inkludert kommunikasjon og samhandling. Informasjonssystemer kan avgrenses mot styrings-/kontrollsystemer.*
Konfidensialitet, integritet og tilgjengelighet	*De tre klassiske målene for informasjonssikkerhet. Konfidensialitet betyr beskyttelse av informasjon mot innsyn fra uautoriserte personer eller prosesser. Integritet betyr beskyttelse av informasjon mot utilsiktet eller uautorisert endring. Tilgjengelighet betyr behovsorientert beskyttelse mot tap eller avbrudd i brukerens autoriserte tilgang til informasjon via en tjeneste eller et system.*
Verdi	*Med verdi menes i det vesentlige liv og helse, økonomiske midler, ytre miljø, bygninger og fasiliteter, infrastruktur, systemer, informasjon eller omdømme. Listen er ikke prioritert eller uttømmende.*
Risiko	*Potensielle (særlig negative) utfall av fremtidige hendelser – med betydning eller innvirkning på virksomhetens eksistens, funksjonsdyktighet eller verdier Risiko knyttet til informasjonssikkerhet gjelder virkningen av usikkerhet på konfidensialitet, integritet og tilgjengelig.*
Sikringstiltak	*Tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger* (NS 5830:2012).
Risikovurdering	*Samlet prosess som består av risikoidentifikasjon, risikoanalyse og risikoevaluering* (SN-ISO Guide 73:2009).
Sektorvist responsmiljø	*Se kbf. § 3-6.*

Uønsket hendelse	*Uønskede hendelser omfatter handlinger, forhold eller andre oppståtte situasjoner som innebærer eller medfører brudd på konfidensialitet, integritet og tilgjengelighet, inkludert kompromittering av sensitiv informasjon, systemfunksjonalitet eller teknologiske sikkerhetstiltak. En uønsket hendelse som forårsakes av en aktør som handler med hensikt er en tilsiktet uønsket handling. Uønskede hendelser kan gi opphav til ekstraordinære situasjoner.*
Hendelseshåndtering	*Aktiviteter med formål om å stanse eller begrense skade på berørte IKT-systemer og nettverksressurser ved sikkerhetstruende hendelser eller handlinger, og deretter gjenopprette sikker tilstand.*
Tjenesteutsetting	*Ekstern utførelse av basisdrift, applikasjonsdrift eller applikasjonsforvaltning, regulert gjennom en kontrakt med en tjenesteleverandør. Tjenesteutsetting, utkontraktering og konkurranseutsetting er likeverdige betegnelser.*
Sikkerhetsrevisjon	*Virksomhetens interne kontroll og kvalitetssikring av eget sikkerhetsarbeid.*

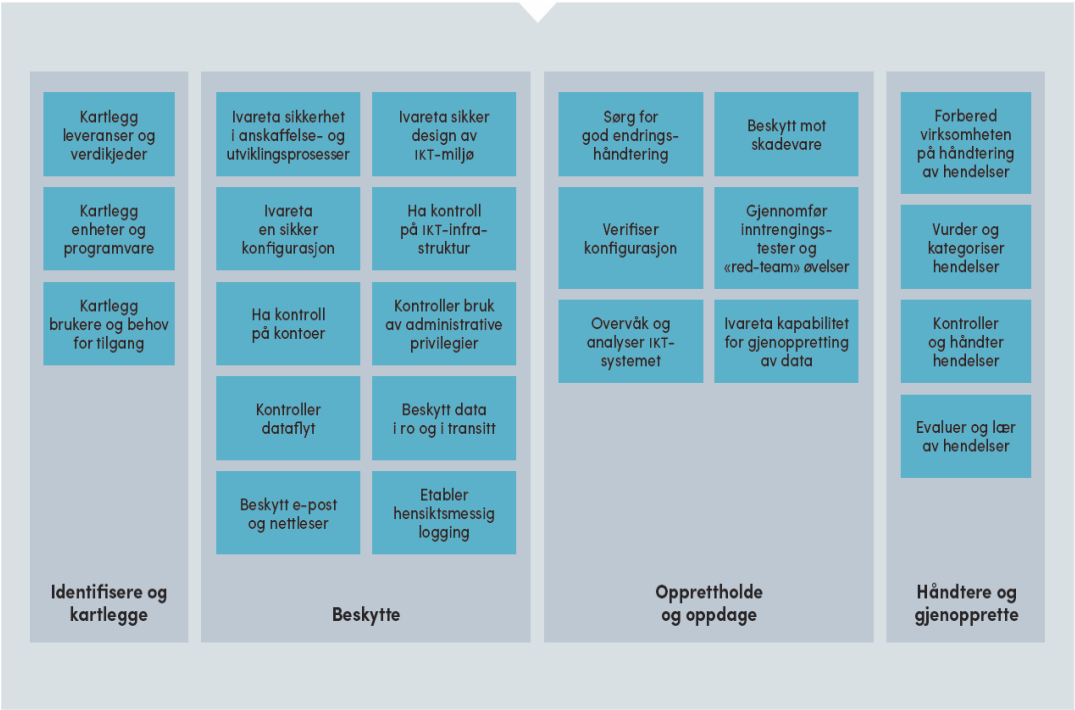
Hvordan kravene kan oppfylles

Sikkerhet bør inngå som en integrert del av virksomhetsprosessene, hvor ansvar og oppgaver for både leder og den enkelte medarbeider er ivaretatt. Kbf § 2-10 stiller krav til internkontrollsystem hos KBO-enheter. Det systematiske sikkerhetsarbeidet innebærer i denne sammenhengen å etablere et styringssystem for informasjonssikkerhet. KBO-enheter har også krav om å utpeke en IKT-sikkerhetskoordinator, se kbf § 2-2c.

Målet for virksomheten bør være kontinuerlig forbedring av sikkerhetstilstanden. Forbedringsarbeid organiseres ofte basert en modell som består av fire trinn: Planlegge, utføre, kontrollere og korrigere.

Forskriften angir krav til de viktigste elementene (i form av aktiviteter og prosesser) i et styringssystem for informasjonssikkerhet. Kravene bygger på NSMs grunnprinsipper for IKT-sikkerhet[9]. NSMs grunnprinsipper for IKT-sikkerhet bygger igjen på internasjonale anerkjente standarder og veiledninger, spesielt ISO/IEC 27002.

[9] https://nsm.stat.no/globalassets/dokumenter/nsm_grunnprinsipper_ikt-sikkerhet_enkeltside_3008.pdf



Figur 1 NSMs grunnprinsipper (Kilde: NSM).

Grunnprinsippene er funksjonsorienterte og gjelder uansett hvilke IKT-driftsmodeller som virksomhetene måtte ha. Implementasjon vil samlet sett gi god beskyttelse av informasjon og digitale systemer. Grunnprinsippene er strukturert i kategorier som representerer grupperinger av logisk beslektede eller avhengige tiltak. Hvert grunn-prinsipp er en kontinuerlig aktivitet som må vurderes i hele systemets levetid, fra planlegging og etablering til avhending. Flere av grunnprinsippene bygger på hverandre, og enkelte er en forutsetning for at andre skal kunne implementeres effektivt. I sum inkluderer grunnprinsippene bredden av sikringstiltak som består av barrierer, deteksjon, verifikasjon og reaksjon for å etablere god sikkerhet i dybden. Tiltakene er relevante også for utilsiktede handlinger, men hovedfokus har vært på tilsiktede.

NSM har et sett med veiledninger som forteller hvordan virksomhetene kan omsette grunnprinsippene til praktisk handling. Der det finnes bransje-, teknologi eller sektor-spesifikt materiale bør dette benyttes i tillegg til de generiske standardene. NVE anbefaler å sette seg inn i NSMs grunnprinsipper og temaveiledninger. Virksomheten kan imidlertid selv velge rammeverk for styring av informasjonssikkerhet.

Relevante rammeverk, standarder og veiledninger for sikkerhetsstyring:

- NSMs veiledning i sikkerhetsstyring
- NSM håndbok i risikovurdering
- NSMs grunnprinsipper for IKT-sikkerhet
- ISO/IEC 27001:2017
- ISO/IEC 27002:2017
- Cyber Essentials
- NIST Cyber Security Framework

Prioritering av tiltak ved etablering av styringssystem må baseres på vurdering av risiko. For IKT-systemer som er eksponert mot Internett kan i første omgang evnen til å oppdage uønsket eller illegitim aktivitet være viktigere enn å beskytte systemer og nettverk. For systemer som håndterer tidskritisk informasjon og allerede er beskyttet kan evnen til å gjenopprette være viktigst.

For større virksomheter med driftskontrollsystemer i klasse 2 og klasse 3 kommer i praksis alle grunnprinsippene under de ulike hovedkategoriene til anvendelse.

Vi henviser til NSMs veiledning(er) for de enkelte grunnprinsippene.

Nedenfor følger en gjennomgang av forskriftskravene i bokstav a-f.

Virksomheten skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer, herunder:

a. Identifisere og dokumentere

Virksomheten skal identifisere og dokumentere verdier, leveranser, tjenester, systemer og brukere i sine digitale informasjonssystemer. Dokumentasjonen skal holdes oppdatert.

Aktiviteten danner grunnlaget for effektiv implementering av de øvrige kravene. Hensikten er å forstå virksomhetens leveranser og tjenester, få oversikt over hvilke teknologiske ressurser som bør sikres, og de roller og brukere virksomheten består av.

I kravet til å *identifisere og dokumentere* inngår følgende grunnprinsipper[10]:

- Kartlegg leveranser og verdikjeder
- Kartlegg enheter og programvare
- Kartlegg brukere og behov for tilgang

Store virksomheter bør implementere samtlige grunnprinsipper og tilhørende tiltak.

b. Risikovurdering

Virksomheten skal gjennomføre risikovurdering ved systemendringer. Risikovurderingen skal holdes oppdatert.

[10] Hentet fra NSMs grunnprinsipper

Risiko skal generelt vurderes for både konfidensialitet, integritet og tilgjengelighet. For kraftsensitiv informasjon er alle sikkerhetsmålene relevante. For målesystemer er typisk integritet og tilgjengelighet viktigere enn konfidensialitet. Risikovurderingen skal kartlegge trusler og fare, og systematisk beskrive forekomst og konsekvens av uønskede hendelser og handlinger.

Risikovurderinger kan ha ulik oppløsning og innretting. Kjente metoder som inngår er grovanalyse, detaljert risiko- og sårbarhetsanalyse i henhold til veiledninger/rammeverk, og bruk av sløyfediagram, hendelsestre og feiltre.

For tilsiktede hendelser må fastsettelse av risiko bygge på en kvalitativ, kunnskapsbasert (subjektiv) vurdering av usikkerhet, noe som ikke alltid kommer frem. Usikkerhet gjelder særlig forekomst av hendelser, men også omfanget av konsekvensene. Risikomatrisen kan representere en uforsvarlig forenkling av virkeligheten dersom ikke usikkerheten kommuniseres. Særlig utfordrende er vurdering av risiko som fremstår med liten sannsynlighet og store konsekvenser. En kartlegging av verdier, trusler og sårbarheter kan med fordel kombineres med en kvalitativ, kunnskapsbasert (subjektiv) vurdering av usikkerhet.

Det er ingen omforent beste fremgangsmåte internasjonalt eller nasjonalt for risiko-vurderinger for tilsiktede uønskede handlinger. Selv om det ikke eksisterer en beste fremgangsmåte, går følgende kjennetegn igjen i en god tilnærming: den (i) er strukturert, (ii) har en arbeidsgruppe med bred kompetanse, (iii) kartlegger kunnskapsstyrken, (iv) er basert på systemforståelse og er konkret, (v) har et helhetlig perspektiv, (vi) kommuniserer risiko og usikkerhet samt (vii) er gjennomsiktig, sporbar og etterprøvbar. (FFI-rapport 2015/00923 s. 3).

Risikovurderinger skal danne beslutningsgrunnlag for iverksetting av risikoreduserende tiltak. Terskelen er virksomhetens aksepterte risiko. Nye risikovurderinger må gjennomføres ved organisatoriske, personellmessige eller systemtekniske endringer som har betydning for informasjonssikkerheten. I tillegg skal har virksomhetens leder ansvar for jevnlig å gjennomføre og revidere risikovurderinger. Risikovurderinger skal gjennomføres av både store og små virksomheter. Dersom tekniske tiltak for å oppnå akseptabel risiko ikke innføres umiddelbart, kan det i en overgangsperiode benyttes administrative tiltak, for eksempel i form av prosedyrer.

Større virksomheter med klassifiserte systemer bør følge en anerkjent standard, veiledning eller norm for risikovurdering. Vi henviser til NSMs *Risikovurdering for sikring*[11], NVEs *Veiledning for risiko- og sårbarhetsanalyser for kraftforsyningen*[12] eller nasjonale (NS 5814:2008 og NS 5832:2014) og internasjonale standarder (spesielt ISO 27000-serien). NB! Trinnene for risikovurdering som beskrives i NS 5814:2008 og NS 5832:2014 er ganske like, selv om termene *risikoanalyse* og *risikovurdering* skiller seg fra hverandre. NVE fraråder den særegne varianten i NS 5832:2014 hvor *(sikrings)-risikoanalyse* omfatter *(sikrings)risikovurdering*.

[11] Håndbok: Risikovurdering for sikring, Publisert: 04.02.2016 | Sist endret: 16.03.2016, https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/risikovurdering-handbok/
[12] Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen, NVE 2010, http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf

c. Sikre og oppdage

Virksomheten skal sikre sine digitale informasjonssystem for å motstå eller begrense skaden fra uønskede hendelser.

Krav til sikring henger sammen med informasjonsverdi, for eksempel kraftsensitiv informasjon (jf. kbf § 6-2), bedriftshemmeligheter, personopplysninger (jf. personopplysningsloven) eller gradert informasjon (jf. sikkerhetsloven). Annen informasjon vil være åpen informasjon.

I kravet til å *sikre* inngår følgende grunnprinsipper[13]:

- Ivareta sikkerhet i anskaffelse- og utviklingsprosesser
- Ivareta sikker design av IKT-miljø
- Ivareta en sikker konfigurasjon (av maskin- og programvare)
- Ha kontroll på IKT-infrastruktur
- Ha kontroll på kontoer
- Kontroller bruk av administrative privilegier
- Kontroller dataflyt
- Beskytt data i ro og i transitt
- Beskytt e-post og nettleser
- Etabler hensiktsmessig logging

For å oppfylle kravet om å sikre, må virksomheten i praksis som et minimum prioritere følgende tiltak:

- Blokkere kjøring av ikke autoriserte programmer
- Oppgradere program- og maskinvare
- Installere sikkerhetsoppdateringer fortløpende
- Begrense tildelingen av administratorrettigheter

Virksomheter skal overvåke sine digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres.

I kravet til å *oppdage* inngår følgende grunnprinsipper[14]

- Sørg for god endringshåndtering
- Beskytt mot skadevare
- Verifiser konfigurasjon
- Gjennomfør inntrengingstester og *red-team*-øvelser.
- Overvåk og analyser IKT-systemet
- Etabler kapabilitet for gjenoppretting av data

Virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer.

Virksomheten skal varsle uønskede hendelser som for eksempel datainnbrudd, nektelses-angrep, oppdagelse av skadevare eller sabotasjeforsøk til det sektorvise responsmiljøet.

[13] NSMs grunnprinsipper
[14] NSMs grunnprinsipper.

NVE tar sikte på å delegere oppgaven med å ta imot slike varsler til KraftCERT. Ekstraordinære situasjoner skal i tillegg varsles og rapporteres til NVE, jf. § 2-5 og § 2-6. Ekstraordinære situasjoner er blant annet situasjoner der konsekvensene er mulige eller faktiske brudd på forskriftens krav til beskyttelse av kraftsensitiv informasjon, kompromittering av driftskontrollsystem og brytefunksjonalitet.

d. Håndtere og gjenopprette

Virksomheten skal håndtere uønskede hendelser i sine digitale informasjonssystemer og gjenopprette normaltilstand uten ugrunnet opphold.

Virksomheten skal ha en prosedyre og en plan for å håndtere sikkerhetsbrudd og gjenopprette systemer og data. Til hendelseshåndtering hører også vurdering av skadeomfang, som er en forutsetning for alle målrettede tiltak. Tiltak og aktiviteter bør dokumenteres underveis, mens evaluering, læring og forbedring er del av oppfølgingen i etterkant av hendelsen.

I kravet til å *håndtere og gjenopprette* inngår følgende grunnprinsipper[15]:

- Forbered virksomheten på håndtering av hendelser
- Vurder og kategoriser hendelser
- Kontroller og håndter hendelser (effektivt)
- Evaluer og lær av hendelser

For anskaffelse av tjenester til hendelseshåndtering henviser vi til NSMs kvalitetsordning[16].

e. Tjenesteutsetting

Virksomheten skal sørge for at sikkerhetsnivået opprettholdes eller forbedres ved utsetting av tjenester.

Forsvarlig tjenesteutsetting innebærer behov for kompetanse på anskaffelse og IKT-sikkerhet. Kompetente rådgivere må hentes inn eksternt dersom virksomheten selv mangler tilstrekkelig kompetanse.

Virksomheten bør dokumentere det eksisterende systemet, inkludert sikkerhetsnivået, før virksomheten går i gang med tjenesteutsetting. Dokumentasjonen bør være så detaljert at det er mulig å kontrollere endringer i system og kompetanse før og etter utsetting.

Virksomheter må velge løsninger som tilbyr minst like god IKT-sikkerhet som eksisterende løsning. I tillegg må løsningen tilfredsstille de andre kravene som forskriften stiller, herunder krav til dokumentasjon, risikovurdering og jevnlig revisjon.

IKT-leverandørindustrien er global og benytter underleverandører i et bredt spekter av land. Virksomheter som planlegger tjenesteutsetting har derfor behov for å vurdere landrisiko for å sørge for at sikkerhetsnivået opprettholdes. GIEK har en nettside med

[15] ibid.
[16] Kvalitetsordning for bruk av leverandørar av tenester for handtering av IKT-hendingar, NSM, https://nsm.stat.no/om-nsm/tjenester/leverandorforhold/kvalitetsordning-for-bruk-av-leverandorer-av-tjenester-innen-ikt-hendelseshandtering/

samlet vurdering av landrisiko for alle land i verden[17], og NSM har utarbeidet en veileder for landrisikovurdering[18]. For tjenesteutsetting av IKT-systemer som behandler kraftsensitiv informasjon (jf § 6-2) gjelder særlige hensyn for å sikre at taushetsplikten ivaretas. Se for øvrig NSMs veileder for tjenesteutsetting[19].

Aktuelle leverandører bør være sertifisert i henhold til én eller flere internasjonalt anerkjente sikkerhetsstandarder. Eksempler på slike er NIST Cyber Security Framework og ISO/IEC 27000-serien. I slike tilfeller bør virksomheten be om å få se tredjeparts revisjonsrapport eller sertifiseringsbevis.

Følgende arbeidsoppgaver inngår ved tjenesteutsetting:

- Dokumentere eksisterende system (jf §6-9 a) og organisasjonens IKT-sikkerhets-kompetanse
- Gjennomføre behovsanalyse
- Vurdere forretningsmodeller for IKT-drift og spesifisere krav til leveranse og leverandør
- Prekvalifisere leverandører, utlyse anbudskonkurranse og gjennomføre eventuelle forhandlingsmøter
- Velge kvalifisert leverandør, gjennomføre kontraktsforhandlinger og inngå kontrakt med kvalifisert(e) leverandør(er)
- Implementere og forvalte ny løsning, og bygge opp nødvendig kompetanse
- Dokumentere nytt system/tjenestemodell, jf. § 6-9 a og ivareta behov for tilgang til IKT-sikkerhetskompetanse
- Avhende eksisterende løsning(er)

f. Sikkerhetsrevisjon

Virksomheter skal jevnlig gjennomføre revisjoner av iverksatte sikringstiltak for digitale informasjonssystemer. Revisjoner skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt. Hver revisjon kan ta for seg deler av sikringstiltakene.

Revisjonsrapporter må være et tema på virksomhetens ledermøter eller andre relevante fora i virksomheten. Som minimum må revisjonen kontrollere organisering av sikkerhets-arbeidet, inkludert plassering av ansvar, og tiltak for beskyttelse av kraftsensitiv informasjon mot uautorisert tilgang. Revisjoner av systemer som er driftet av ekstern leverandør, bør omfatte kontroll av tredjepartsrevisjon og -sertifiseringer.

Resultatene og konklusjonene fra sikkerhetsrevisjonene må dokumenteres. Avvik og feil må håndteres i henhold til virksomhetens internkontrollsystem jf. kbf. § 2-10.

[17] https://www.giek.no/landrisiko/
[18] Anbefaling om landvurdering ved tjenesteutsetting, NSM (2018) https://nsm.stat.no/globalassets/dokumenter/temahefter/anbefaling-om-landvurdering-ved-tjenesteutsetting.pdf
[19] Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området *Beslutt leveransemodell* i NSMs grunnsprinsipper for IKT-sikkerhet, https://nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_web.pdf

§ 6-10. Brytefunksjonalitet i AMS

§ 6-10. ***Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)***

Nettselskap som har avanserte måle- og styringssystem (AMS) med brytefunksjonalitet, skal sikre dette mot uønsket tilgang. Brytefunksjonalitet som definert i forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. § 1-3, inkluderer i denne bestemmelsen begrensning av energi- og effektuttaket i det enkelte målepunkt. Nettselskap skal etablere og opprettholde egne sikkerhetstiltak for brytefunksjonaliteten, herunder:

a. Det er kun nettselskap som har tillatelse til å utføre fjernstyring av bryte-funksjonaliteten. Fjernstyring av brytefunksjonaliteten skal utføres fra en adgangskontrollert sone.

b. Leverandør med fjerntilgang til brytefunksjonaliteten, skal være lokalisert i et land som er medlem i EFTA, EU eller NATO. Leverandør lokalisert i andre land kan få tidsavgrenset fjerntilgang til brytefunksjonalitet under løpende oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra leverandør lokalisert i land som er medlem i EFTA, EU eller NATO.

   Før leverandør lokalisert i land utenfor EFTA, EU eller NATO får fjerntilgang til brytefunksjonaliteten, skal nettselskapet foreta en risikovurdering som inneholder en vurdering av landrisiko.

c. Nettselskap har ansvar for at det etableres kontrollordninger for bruk av bryte- og oppdateringsfunksjonaliteten som hindrer at en enkelt person eller enkelt bruker kan koble ut flere målepunkt samtidig.

d. Fjernoppdatering av programvaren i AMS skal utføres fra en adgangskontrollert sone hos nettselskap eller leverandør. Ved bruk av leverandør skal vilkårene i bokstav b være oppfylt.

e. Hver enkelt måler skal ha en individuell sikkerhetsløsning for bryte-, og oppdaterings-funksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler.

Hvorfor vi har bestemmelsen

Formålet er å for det første å sette tydelige krav til sikring av brytefunksjonalitet hos nettselskapet. For det andre er formålet å klargjøre at det er nettselskapene som er ansvarlige.

Bakgrunnen er økt risiko for vidtrekkende feil eller uautorisert inntrenging som følge av digitalisering og sammenkobling av systemer. Målerne har en innebygget funksjon for bryting av strøm. Bestemmelsen skal bidra til å redusere risikoen for at denne funksjonen er tilgjengelig for uautoriserte brukere og at funksjonen blir misbrukt. Bestemmelsen bygger på kravene til sikring av digitale informasjonssystemer i kbf § 6-9.

Hvem bestemmelsen gjelder for

Bestemmelsen nettselskap som har AMS med brytefunksjonalitet. Det vil i praksis si KBO-enheter.

Ordforklaringer

Ord	Forklaring
Avanserte måle- og styringssystem (AMS)	*Toveis informasjons- og kommunikasjonssystem fra og med elektrisitetsmålere benyttet til avregning for de enkelte målepunkt, til og med sentralsystemet hos nettselskap eller nettselskapets leverandør* (maf. § 1-3).
Brytefunksjonalitet	*System for fjernstyrt inn- og utkobling av strømuttaket i målepunktet til AMS-målere Dette inkluderer begrensning av energi og effektuttak i det enkelte målepunkt.*
Adgangskontrollert sone	*En adgangskontrollert sone (eller område) er et avgrenset og fysisk sikret rom, del av bygning eller bygning med styrt og kontrollert adgang. Virksomheten skal kunne gjøre rede for hvem som har vært inne i sonen.*
Fjerntilgang	*Tilgang til IKT-system fra en fysisk lokasjon utenfor anlegget der IKT-systemets maskinvare befinner seg.*
Fjernstyring	*Styring som skjer over en geografisk avstand.*
Kontrollordninger	*Tekniske sikkerhetstiltak, sikkerhetsmekanismer og prosedyrer.*

Hvordan kravene kan oppfylles

AMS er et digitalt informasjonssystem og kravene til grunnsikring i kbf § 6-9 gjelder derfor også for sikring av den logiske kjeden og kommandoer fra virksomhetens sentralsystem (head-end), gjennom nettverket og fram til brytefunksjonen i måleren. Vi viser til omtale under kbf § 6-9.

a. *Det er kun nettselskap som har tillatelse til å utføre fjernstyring av brytefunksjonaliteten. Fjernstyring av brytefunksjonaliteten skal utføres fra en adgangskontrollert sone.*

Det er ingen andre enn nettselskap som kan kople inn eller ut strøm til kunder. Ut- eller innkopling må kun skje fra adgangskontrollert sone der det er fysisk kontroll med hvem som har adgang, og der kun personell med legitimt behov har adgang. Hotellrom vil ikke være adgangskontrollert sone fordi en ikke har kontroll med hvem som besøker dette rommet.

b. *Leverandør med fjerntilgang til brytefunksjonaliteten, skal være lokalisert i et land som er medlem i EFTA, EU eller NATO. Leverandør lokalisert i andre land kan få tidsavgrenset fjerntilgang til brytefunksjonalitet under løpende oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra leverandør*

lokalisert i land som er medlem i EFTA, EU eller NATO.

Før leverandør utenfor EFTA, EU eller NATO får tilgang til brytefunksjonaliteten, skal nettselskapet foreta en risikovurdering som inneholder en vurdering av landrisiko.

Uønsket tilgang til brytefunksjonaliteten kan få like vidtrekkende konsekvenser for forsyning av elektrisitet til strømkunder som uønsket tilgang til og manipulasjon av driftskontrollsystemer. Kravet er derfor harmonisert med § 7-14 k.

Dersom nettselskapet har behov for å gi leverandører utenfor EFTA, EU eller NATO tilgang, må selskapet gjøre en landrisikovurdering og iverksette nødvendige sikringstiltak. Se punkt e *Tjenesteutsetting*. Leverandører med fjerntilgang til brytefunksjonaliteten må til enhver tid være under oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra en leverandør som er lokalisert i land som er medlem i EFTA, EU eller NATO. Med oppsyn menes kontinuerlig observasjon. Med kvalifisert personell menes personell med tilstrekkelig kompetanse til å forstå arbeidsoperasjonen som blir gjennomført.

c. *Nettselskap har ansvar for at det etableres kontrollordninger for bruk av bryte- og oppdateringsfunksjonaliteten som hindrer at en enkelt person eller enkelt bruker kan koble ut flere målepunkt samtidig.*

Aktuelle kontrollordninger kan være:

- Tilgangskontroll
- Separering av rettigheter (separation of duties)
- Flerfaktor-autentisering
- Logging og etterkontroll av logger
- Reaksjoner på brudd på rutinene som for eksempel sikkerhetssamtale eller oppsigelse

d. *Fjernoppdatering av programvaren i AMS skal utføres fra en adgangskontrollert sone hos nettselskap eller leverandør. Ved bruk av leverandør skal vilkårene i bokstav b være oppfylt.*

Kravet kommer i tillegg til sikring av digitale informasjonssystemer, jf. kbf § 6-9.
NVE viser til forklaring av adgangskontrollert sone og til bokstav b ovenfor.

e. *Hver enkelt måler skal ha en individuell sikkerhetsløsning for bryte-, og oppdateringsfunksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler.*

Ingen som får kontroll over en måler, og som kan lese av innholdet i den, skal alene kunne bruke kontrollen og/eller informasjonen til å endre innstillingene i sentralsystemet, AMS-målere, eller andre deler av infrastrukturen. Hver måler må ha innebygget sikkerhetsløsning som forhindrer at brytefunksjonaliteten blir misbrukt.

7 Endringer i kapittel 7

§ 7-1. Generell plikt til å beskytte driftskontrollsystemet

§ 7-1. ***Generell plikt til å beskytte driftskontrollsystemet***

Virksomheter med driftskontrollsystem skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser

Driftskontrollsystemer omfatter driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner. Med anlegg forstås også tilhørende bygningstekniske konstruksjoner for driftskontrollfunksjoner.

Driftskontrollfunksjoner er alle organisatoriske, administrative og tekniske tiltak for å overvåke, styre og beskytte anlegg i kraftforsyningen.

Det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.

Hvorfor vi har bestemmelsen

Formålet er å sikre at driftskontrollsystemet skal virke til enhver tid, at det er tydelig hva et driftskontrollsystem omfatter og hva driftskontrollfunksjoner er.

Driftskontrollsystemer er kritiske for forsyningssikkerhet og HMS. Styring og drift skal også kunne utføres under ekstraordinære situasjoner.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet ledd.

Ordforklaringer

Ord	**Forklaring**
Sambandsanlegg	*Anlegg for overføring av informasjon, tale, data og signaler.*
Utstyr	*Verktøy, maskiner, reparasjonsmateriell og komponenter som er nødvendig for å foreta reparasjoner, gjenoppretting eller midlertidige tiltak. Utstyr som er nødvendig for at sentralen kan tjene som et rom for betjeningen som utøver styring og overvåkning på døgnbasis.*

Hvordan kravene kan oppfylles

Virksomheter med driftskontrollsystem skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser

For å kunne sørge for at driftskontrollsystemet til enhver tid virker etter sin hensikt, og beskytte mot alle typer uønskede hendelser er det nødvendig med en risikovurdering av hele driftskontrollsystemet.

Det er viktig å forstå sårbarhetene i systemet dersom det utsettes for uønskede hendelser. Dette gjelder særlig spesielt store eller omfattende hendelser som kan sette systemet ut av spill i lengre tid. Når det gjelder hvilke risikovurderinger som bør gjøres for et driftskontrollsystem, viser NVE til veileder 1/2013 til tidligere § 7-1.

Bestemmelsen om rapportering i § 2-6 angir en liste med av uønskede hendelser virksomhetene skal rapportere. Denne listen må ses som et minimum av hendelser virksomheten skal beskytte driftskontrollsystemet mot.

Det tillates ikke at eksterne leverandører som ikke er KBO-enhet, utfører driftskontrollfunksjoner i nettanlegg eller produksjonsanlegg.

Flere tekniske tiltak og prosedyrer tiltak kan bidra til å forhindre at leverandører med tilgang til driftskontrollsystemet uforvarende eller bevist styrer anlegg. Eksempler på tiltak er:

- Seksjonering av nett, eksempelvis eget servicenett for leverandører,
- Begrensning av tilgangsrettigheter, hvem som har tilgang til å skrive, modifisere eller lese data, samt tidsrom rettighetene gjelder for
- Kontroll av datatrafikk og deteksjonsmekanismer for unormal aktivitet
- Logging og overvåkning av leverandørens operasjoner

Feilretting i driftskontrollsystemet anses ikke som utøvelse av driftskontrollfunksjoner, og forhindres derfor ikke av denne bestemmelsen. Slik tilgang er beskrevet i §7-10 ekstern tilkobling til driftskontrollsystem.

§ 7-10. Ekstern tilkobling til driftskontrollsystemet

§ 7-10. ***Ekstern tilkobling til driftskontrollsystem***

Virksomheter skal ha kontroll med ekstern tilkobling til driftskontrollsystemet.

Kun godkjente brukere kan gis tilgang til driftskontrollsystemet gjennom ekstern tilkobling. Virksomheter skal ha en oppdatert liste over alle godkjente brukere.

Det skal foreligge en egen forhåndsavtalt prosedyre for ekstern tilkobling til driftskontrollsystemet.

Virksomheter skal ha kontrollordninger for å godkjenne, vedlikeholde og avvikle ordninger for ekstern tilkobling til driftskontrollsystemet, og for funksjoner for innstilling av vern.

Virksomheter skal ha kontrollordninger for vurdering, tildeling, endring og tilbaketrekking av brukertilgang.

Hvorfor vi har bestemmelsen

Formålet er å redusere risiko for å introdusere skadelig programvare og feil når leverandører knytter seg til systemet for å vedlikeholde eller utføre service og reparasjoner.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet ledd.

Hvordan kravene kan oppfylles

Virksomheten oppfyller kravene gjennom å:

- Separere nettverket for driftskontrollsystemet i sikkerhetsdomener i henhold til rettigheter og oppgaver. Som minimum skal overvåkning og vedlikehold gjøres via et eget nettverkssegment (servicenett).
- Etablere prosedyrer og kriterier for tilgangsstyring, som blant annet omhandler tildeling av rettigheter, bruk av protokoller, oppsett av tilgangspunkter og metoder for autentisering.
- Vedlikeholde oversikt over hvilke brukere og prosesser som er tildelt roller og rettigheter for de ulike komponentene/delsystemene i driftskontrollsystemet.
- Gjennomfør aktivitetslogging og -rapportering for alle fjernpåloggingssesjoner (ref. NVEs rapport om logging for mer detaljert informasjon).
- Jevnlig gå gjennom tildelte tilgangsrettigheter ved å kontrollere at alle brukere har korrekt tilgangsnivå. Virksomheten må også kontrollere at eventuelle endringer og slettinger er gjennomført.

§ 7-14. Særskilte krav til driftskontrollsystem i klasse 2

§ 7-14. ***Særskilte krav til driftskontrollsystem klasse 2*, bokstav f:**

f. Ekstern tilkobling til driftskontrollsystemet

Ved tilkobling fra leverandører skal driftssentralen være bemannet.

Virksomheter skal ha kontrollordning for korrekt verifisering av de brukere som er *godkjent* til å benytte ekstern tilkobling for tilgang til driftskontrollsystemet. Det er ikke tillatt at én brukeridentitet deles mellom flere personer eller systemer.

Virksomheter skal sørge for at ekstern tilkobling utføres fra et sted med tilstrekkelig sikre omgivelser. Virksomheter 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 *kraft*forsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person.

Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

I § 7-14. *Særskilte krav til driftskontrollsystem klasse 2*, bokstav k:

k. Krav til leverandører

For leveranser til driftskontrollsystemer tillates kun utenlandske leverandører fra land som er medlem i EFTA, EU eller NATO. En leveranse omfatter levering av utstyr, komponenter, programvare, data, programmeringstjenester, oppdateringer, feilretting, service og vedlikehold.

Hvorfor vi har bestemmelsen

Formålet er å sørge for et tilstrekkelig sikkerhetsnivå for driftskontrollsystemer i klasse 2.

Hvem bestemmelsen gjelder for

KBO-enheter og andre virksomheter med vedtak etter § 1-3 annet ledd.

Hvordan kravene kan oppfylles

§ 7-14 f Ekstern tilkobling til driftskontrollsystemet

§ 7-14 f presiserer kravene for tilkopling til driftskontrollsystem klasse 2. Kravene gjelder både for KBO-enheter og leverandører. Kravene er selvforklarende og gjengis ikke her.

§ 7-14 k Krav til leverandører

Ved leveranser til driftskontrollsystem i klasse 2 må det gjennomføres en risikovurdering hvor leverandørens tilholdssted skal være en del av vurderingen, jf. § 2-3 og § 5-8.

Utenlandske leverandører må komme fra land som er medlem av EFTA, EU eller NATO. Leverandører som i dag leverer driftskontrollsystemer, er plassert i land som er medlem av NATO, EU og/eller EFTA.

Om det skulle oppstå et særskilt behov for anskaffelser fra andre land, må virksomheten søke dispensasjon etter § 8-3. En slik dispensasjonssøknad må blant annet inneholde en vurdering av landrisiko. Dette vil også omfatte f.eks. komponenter for driftskontrollfunksjoner.

8 Bibliografi

Datatilsynet. (2018). *Kredittvurdering.* Hentet fra www.datatilsynet.no: https://www.datatilsynet.no/personvern-pa-ulike-omrader/kundehandtering-handel-og-medlemskap/kredittvurdering/

Forsvarets forskningsinstitutt. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* Kjeller: FFI.

Garantiinstituttet for eksportkreditt. (u.d.). *Landrisiko*. Hentet fra www.giek.no: https://www.giek.no/landrisiko/

ISO/IEC. (2017). *ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry, .* Hentet fra www.standard.no: https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=946514

Nasjonal sikkerhetsmyndighet. (2016). *Håndbok: Risikovurdering for sikring*. Hentet fra nsm.stat.no: https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/risikovurdering-handbok/

Nasjonal sikkerhetsmyndighet. (2016). *NSMs grunnprinsipper for IKT-sikkerhet. Versjon 1.0.* Oslo: Nasjonal sikkerhetsmyndighet (NSM).

Nasjonal sikkerhetsmyndighet. (2016). *Risikovurdering for sikring*. Hentet fra www.nsm.stat.no: https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf

Nasjonal sikkerhetsmyndighet. (2017). *Beskrivelse av grunnleggende tiltak for sikring av overføring av epost mellom e-posttjenere*. Hentet fra www.nsm.stat.no: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/u-02-grunnleggende-tiltak-for-sikring-av-e-post---endelig.pdf

Nasjonal sikkerhetsmyndighet. (2017). *Logging. Økt sikkerhet i IKT-systemer*. Hentet fra www.nsm.stat.no: https://nsm.stat.no/globalassets/dokumenter/temahefter/logging-for-okt-sikkerhet-i-ikt-systemer_2017.pdf

Nasjonal sikkerhetsmyndighet. (2017). *Rammeverk for ha ndtering av IKT-sikkerhetshendelser. Versjon 07.12.2017.* Oslo: Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet. (2018). *Anbefaling om landvurdering ved tjenesteutsetting*. Hentet fra nsm.stat.no: https://nsm.stat.no/globalassets/dokumenter/temahefter/anbefaling-om-landvurdering-ved-tjenesteutsetting.pdf

Nasjonal sikkerhetsmyndighet. (2018). *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området «Beslutt leveransemodell» i NSMs grunnsprinsipper for IKT-sikkerhet*. Hentet fra www.nsm.stat.no: Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området «Beslutt leveransemodell» i NSMs grunnsprinsipper fhttps://nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_web.pdf

Nasjonal sikkerhetsmyndighet. (2018, 08 29). *www.nsm.stat.no*. Hentet fra Rammeverk for håndtering av IKT-hendelser: https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

Nasjonal sikkerhetsmyndighet. (u.d.). *Kvalitetsordning for bruk av leverandørar av tenester for handtering av IKT-hendingar*. Hentet fra www.nsm.stat.no: https://nsm.stat.no/om-nsm/tjenester/leverandorforhold/kvalitetsordning-for-bruk-av-leverandorer-av-tjenester-innen-ikt-hendelseshandtering/

National Cyber Security Centre. (u.d.). *Cyber essentials: Protect your organisation against cyber attack*. Hentet fra https://www.cyberessentials.ncsc.gov.uk/: https://www.cyberessentials.ncsc.gov.uk/

National Institute for Standards and Technology. (u.d.). *Cybersecurity Framework*. Hentet fra https://www.nist.gov/cyberframework: https://www.nist.gov/cyberframework

Norges vassdrags- og energidirektorat. (2010). *Veiledning i risiko- og sårbarhetsanalyse*. Hentet fra www.nve.no: http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf

Norges vassdrags- og energidirektorat. (2017). *Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem. Rapport utarbeidet av BDO AS for Norges vassdrags- og energidirektorat, NVE Rapport 14:2017*. Hentet fra www.nve.no: http://publikasjoner.nve.no/rapport/2017/rapport2017_14.pdf

Norsk senter for informasjonssikring. (2018). *Sikring av mobile enheter*. Hentet fra www.norsis.no: https://norsis.no/sikring-av-mobile-enheter-ouch-nyhetsbrev/

North America Electric Reliability Corporation. (u.d.). *Cyber Security (Permanent)* . Hentet fra www.nerc.com: https://www.nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx

Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet og Næringslivets Sikkerhetsråd. (2017). *Sikkerhet ved ansettelsesforhold - før, under og ved avvikling.* Hentet fra www.nsm.stat.no: https://nsm.stat.no/globalassets/dokumenter/veiledninger/sikkerhet_ved

Standard Norge. (2008). *NS 5814:2008 Krav til risikovurderinger.*

Standard Norge. (2009). *SN-ISO Guide 73:2009 Risikostyring - Terminologi.*

Standard Norge. (2012). *NS 5830:2012 Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi* .

Standard Norge. (2014). *NS 5832:2014 Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse* .

VEDLEGG 1

KBF	Tilleggsveileder	Veileder 1/2013	Tilsvarende BFE
§ 1-1 Formål		X	§ 1-1. Formål
§ 1-2 Virkeområde		X	§ 1-2. Virkeområde
§ 1-3 Hvem forskriften gjelder for	X		§ 1-3. Hvem forskriften er rettet mot
§ 1-4 Ansvar		X	§ 2-1. Ansvar
§ 1-5 Beredskapsplikt og bereskapsplan		X	§ 2-3. Beredskapsplikt
§ 2-1 Kraftforsyningens beredskapsorganisasjon		X	§ 3-1. Organisering av KBO og § 3-3. KBO-enheter
§ 2-2 Organisasjon og funksjon	X	X	§ 2-2. Organisasjon og funksjon
§ 2-3 Risikovurdering		X	§ 2-4. Risiko- og sårbarhetsanalyse
§ 2-4 Beredskapsplanlegging		X	§ 2-5. Beredskapsplanlegging
§ 2-5. Varsling	X	X	§ 2-6. Varsling og rapportering
§ 2-6. Rapportering	X	X	§ 2-6. Varsling og rapportering
§ 2-7 Øvelser		X	§ 2-7. Øvelser
§ 2-8 Informasjonsberedskap		X	§ 2-8. Informasjonsberedskap
§ 2-9 Evaluering		X	§ 2-9. Evaluering
§ 2-10 Internkontrollsystem		X	§ 2-10. Internkontrollsystem
§ 3-1 Beredskapsmyndigheten		X	§ 3-2. Beredskapsmyndigheten
§ 3-2 Ansvar og oppgaver for KBO-enhetene		X	§ 3-3. KBO-enheter
§ 3-3 Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig		X	§ 3-5. Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig
§ 3-4 Ansvar og oppgaver for KDS		X	§ 3-6. Ansvar og oppgaver for kraftforsyningens distriktssjefer
§ 3-5 Fritaksordninger		X	§ 3-7. Fritaksordninger
§ 3-6 Sektorvist responsmiljø for IKT-sikkerhetshendelser	X		NY
§ 4-1 Reperasjonsberedskap		X	§ 4-1 Reperasjonsberedskap
§ 4-2 Kompetanse og personell		X	§ 4-2 Kompetanse og personell
§ 4-3 Drift i ekstraordinært situasjoner og gjenoppretting av funksjon		X	§ 4-3 Drift i ekstraordinært situasjoner og gjenoppretting av funksjon
§ 4-4 Materiell og utstyr		X	§ 4-4 Materiell og utstyr
§ 4-5 Transport		X	§ 4-5 Transport
§ 4-6 Nasjonal tungtransportberedskap		X	§ 4-6 Nasjonal tungtransportberedskap
§ 4-7 Samband		X	§ 4-7 Samband
§ 5-1. Sikringsplikt		X	§ 5-1. Sikringsplikt
§ 5-2. Klasser	X	X	§ 5-2. Klasser
§ 5-3. Sikring av klassifiserte anlegg		X	§ 5-3. Sikring av klassifiserte anlegg
§ 5-4. Sikringstiltak for klasse 1		X	§ 5-4. Sikringstiltak for klasse 1
§ 5-5. Sikringstiltak for klasse 2		X	§ 5-5. Sikringstiltak for klasse 2
§ 5-6. Sikringstiltak for klasse 3		X	§ 5-6. Sikringstiltak for klasse 3
§ 5-7. Vedtak om sikring eller klasse		X	§ 5-7. Vedtak om sikring eller klasse
§ 5-8. Vurdering		X	§ 5-8. Analyse
§ 5-9. Meldeplikt om sikringstiltak	X		§ 5-9. Meldeplikt om sikringstiltak
§ 5-10. Vakthold		X	§ 5-10. Vakthold
§ 5-11. Restriksjoner for adgang til steder og områder	X	X	§ 5-11. Besøksrestriksjoner
§ 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere	X	X	§ 6-1. Identifisering av sensitiv informasjon og rettmessige brukere
§ 6-2. Kraftsensitiv informasjon	X	X	§ 6-2 Sensitiv informasjon
§ 6-3. Beskyttelse, avskjerming og tilgangskontroll	X	X	§ 6-3 Beskyttelse, avskjerming og tilgangskontroll
§ 6-4. Sikkerhetsinstruks	X	X	§ 6-4. Sikkerhetsinstruks
§ 6-5. Anskaffelser	X	X	§ 6-5. Anskaffelser i energiforsyningen
§ 6-6. Begrenset anbudsinnbydelse		X	§ 6-6. Begrenset anbudsinnbydelse

§ 6-7. Personkontroll	X		NY
§ 6-8. Sikkerhetskopier		X	§ 6-8. Sikkerhetskopier
§ 6-9. Digitale informasjonssystemer	X		NY
§ 6-10.Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)	X		NY
§ 7-1. Generell plikt til å beskytte driftskontrollsystemet	X		§ 7-1. Generell plikt til å beskytte driftskontrollsystemet
§ 7-2. Interne sikkerhetsregler		X	§ 7-2. Interne sikkerhetsregler
§ 7-3. Dokumentasjon av driftskontrollsystemet		X	§ 7-3. Dokumentasjon av driftskontrollsystemet
§ 7-4. Kontroll med brukertilgang		X	§ 7-4. Kontroll med brukertilgang
§ 7-5. Kontroll ved endringer i dritskontrollsystemet		X	§ 7-5. Kontroll ved endringer i dritskontrollsystemet
§ 7-6. Kontroll med utstyr i driftskontrollsystemet		X	§ 7-6. Kontroll med utstyr i driftskontrollsystemet
§ 7-7. Håntering av feil, sårbarheter og sikkerhetsbrudd		X	§7-7. Håntering av feil, sårbarheter og sikkerhetsbrudd
§ 7-8. Beredskap ved svikt i driftskontrollsystemet		X	§ 7-8. Beredskap ved svikt i driftskontrollsystemet
§ 7-9. Bemanning av driftssentral		X	§ 7-9. Bemanning av driftssentral
§ 7-10. Ekstern tilkobling til driftskontrollsystem	X		§ 7-10. Ekstern tilkobling til driftskontrollsystem
§ 7-11. Systemredundans i driftskontrollsystemet		X	§ 7-11. Systemredundans i driftskontrollsystemet
§ 7-12. OPPHEVES			§ 7-12. Sammenkobling mellom avsanserte måle- og styringssystem og driftskontrollsystem
§ 7-13. Beskyttelse mot elektromagnetisk puls og inferens		X	§ 7-13. Beskyttelse mot elektromagnetisk puls og inferens
§ 7-14. Særskilte krav til driftskontrollsystemt i klasse 2	X	X	§ 7-14. Særskilte krav til driftskontrollsystemt i klasse 2
§ 7-15. Særskitle krav til driftskontrollsystem i klasse 3		X	§ 7-15. Særskitle krav til driftskontrollsystem i klasse 3
§ 7-16. Vern av kraftsystem i regional- og transmisjonsnett		X	§ 7-16. Vern av kraftssystem i regional- og sentralnett
§ 7-17.Mobile radionett - driftsradio		X	§ 7-17.Mobile radionett - driftsradio
§. 8-1. Kontroll		X	§. 8-1. Kontroll
§. 8-2. Pålegg		X	§. 8-2. Pålegg
§. 8-3. Dispensasjon		X	§. 8-3. Dispensasjon
§ 8-4. Tvangsmulkt		X	§ 8-4. Tvangsmulkt
§ 8-5. Overtredelsesgebyr		X	§ 8-5. Overtredelsesgebyr
§ 8-6. Straff		X	§ 8-6. Straff
§. 8-7. Gebyr til beredskapsmyndigheten		X	§. 8-7. Gebyr til beredskapsmyndigheten
§ 8-8. Forholdet til eldre vedtak om klassifisering og overgangsregler		X	§ 8-8. Forholdet til eldre vedtak om klassifisering og overgangsregler

VEDLEGG 2

BESTEMMELSENE	KBO-enhet	Virksomheter med vedtak etter § 1-3 annet ledd	Virksomheter med vedtak etter § 1-3 tredje ledd	Enhver
§ 1-1. Formål				
§ 1-2. Virkeområde				
§ 1-3. Hvem forskriften gjelder for				
§ 1-4. Ansvar	X	X		
§ 1-5. Beredskapsplikt og bereskapsplan	X	X		
§ 2-1. Kraftforsyningens beredskapsorganisasjon	X			
§ 2-2. Organisasjon og funksjon	X			
§ 2-3 Risikovurdering	X			
§ 2-4. Beredskapsplanlegging	X			
§ 2-5. Varsling	X			
§ 2-6. Rapportering	X			
§ 2-7. Øvelser	X			
§ 2-8. Informasjonsberedskap	X			
§ 2-9. Evaluering	X			
§ 2-10. Internkontrollsystem	X			
§ 3-1. Beredskapsmyndigheten				
§ 3-2. Ansvar og oppgaver for KBO-enhetene	X			
§ 3-3. Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig	X			
§ 3-4. Ansvar og oppgaver for KDS				
§ 3-5. Fritaksordninger	x			
§ 3-6. Sektorvist responsmiljø for IKT-sikkerhetshendelser				
§ 4-1. Reperasjonsberedskap	X			
§ 4-2. Kompetanse og personell	X			
§ 4-3. Drift i ekstraordinære situasjoner og gjenoppretting av funksjon	X			
§ 4-4. Materiell og utstyr	X			
§ 4-5. Transport	X			
§ 4-6. Nasjonal tungtransportberedskap	X			
§ 4-7. Samband	X			
§ 5-1. Sikringsplikt	X	X		
§ 5-2. Klasser	X			
§ 5-3. Sikring av klassifiserte anlegg	X			
§ 5-4. Sikringstiltak for klasse 1	X			
§ 5-5. Sikringstiltak for klasse 2	X			
§ 5-6. Sikringstiltak for klasse 3	X			
§ 5-7. Vedtak om sikring eller klasse				
§ 5-8. Vurdering	X	X		

§ 5-9. Meldeplikt om sikringstiltak	X	X		
§ 5-10. Vakthold	X	X		
§ 5-11. Restriksjoner for adgang til steder og områder	X			
§ 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere	X	Fjerde ledd	Fjerde ledd	Fjerde ledd
§ 6-2. Kraftsensitiv informasjon	X	X	X	X
§ 6-3. Beskyttelse, avskjerming og tilgangskontroll	X	X	X	
§ 6-4. Sikkerhetsinstruks	X	X	X	
§ 6-5. Anskaffelser	X			
§ 6-6. Begrenset anbudsinnbydelse	X			
§ 6-7. Personkontroll	X			
§ 6-8. Sikkerhetskopier	X	X		
§ 6-9. Digitale informasjonssystemer	X	X		
§ 6-10.Brytefunksjonalitet i avanserte måle- og styringssystem (AMS)	X			
§ 7-1. Generell plikt til å beskytte driftskontrollsystemet	X	X		
§ 7-2. Interne sikkerhetsregler	X	X		
§ 7-3. Dokumentasjon av driftskontrollsystemet	X	X		
§ 7-4. Kontroll med brukertilgang	X	X		
§ 7-5. Kontroll ved endringer i dritskontrollsystemet	X	X		
§ 7-6. Kontroll med utstyr i driftskontrollsystemet	X	X		
§ 7-7. Håntering av feil, sårbarheter og sikkerhetsbrudd	X	X		
§ 7-8. Beredskap ved svikt i driftskontrollsystemet	X	X		
§ 7-9. Bemanning av driftssentral	X	X		
§ 7-10. Ekstern tilkobling til driftskontrollsystem	X	X		
§ 7-11. Systemredundans i driftskontrollsystemet	X	X		
§ 7-12. OPPHEVES				
§ 7-13. Beskyttelse mot elektromagnetisk puls og inferens	X	X		
§ 7-14. Særskilte krav til driftskontrollsystemt i klasse 2	X			
§ 7-15. Særskitle krav til driftskontrollsystem i klasse 3	X			
§ 7-16. Vern av kraftsystem i regional- og transmisjonsnett	X			
§ 7-17.Mobile radionett - driftsradio	X			
§ 8-1. Kontroll	X	X		
§ 8-2. Pålegg (vedtakshjemmel)				
§ 8-3. Dispensasjon (vedtakshjemmel)				
§ 8-4. Tvangsmulkt (vedtakshjemmel)				
§ 8-5. Overtredelsesgebyr (vedtakshjemmel)				
§ 8-6. Straff (vedtakshjemmel)				
§ 8-7. Gebyr til beredskapsmyndigheten				
§ 8-8. Forholdet til eldre vedtak om klassifisering og overgangsregler				