



NVE

NY KRAFTBEREDSKAPSFORSKRIFT (KBF)

Seminar 28.11.2018

Ingunn Åsgard Bendiksen
Direktør, Tilsyns- og beredskapsavdelingen NVE



Hvorfor endringer?

- Forebyggende sikkerhet og beredskap i kraftforsyningen stadig viktigere
- Fornyelse – gjeldende forskrift vedtatt 2012
- Forbedringer - eks nye krav IKT-sikkerhet, begrepsbruk mm
- Forenklinger – eks klassifisering
- Ny sikkerhetslov med forskrifter i kraft fra 1.1.2019

Nye trusler gir endringsbehov



Forskriftsdokumenter og veiledere





Beredskapstilsyn 2019 - revisjoner

Reparasjonsberedskap 132 kV GIS-anlegg	2
Reparasjonsberedskap transformator	2
Reparasjonsberedskap vannkraftverk	3
Sikringstiltak transformatorstasjoner	8
Sikringstiltak driftssentraler	1
Driftskontroll/IKT	5
AMS	1
Informasjonssikkerhet	5
Lynoverspenninger/jording	3
Generelt beredskapstilsyn vindkraftverk	1
Generelt beredskapstilsyn/vedlikehold	13
Generelt beredskapstilsyn/vedlikehold/rasjonering	3
Generelt beredskapstilsyn, fjernvarme	4
Felles tilsyn med NKOM	1
Felles tilsyn med DSB. Lynoverspenninger/jording	3



Informasjon, kompetansebygging og kurs

- KDS-møter og andre arenaer
- NTNU CCIS EVU-kurs
- EnergiNorge i samarbeid med NSM og NTNU CCIS
- CyberSmart
- Energiberedskap 2019 i Drammen 22. – 23. mai



Foto: Pixabay



NVE

KBF: KAPITTEL 1-3

Eldri Naadland Holo
Seksjonssjef TBB

Kapittel I.

Innledende bestemmelser



Kapittel 1. Innledende bestemmelser

- § 1-2. Virkeområde
 - Forskriften gjelder forebygging, håndtering og begrensnig av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring og fordeling av elektrisk energi eller fjernvarme.
- § 1-2. Virkeområde
 - Forskriften gjelder forebygging, håndtering og begrensnig av virkningene av ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi eller fjernvarme.



Kapittel 1. Innledende bestemmelser

- § 1-3. *Hvem forskriften er rettet mot*
- Forskriften gjelder for de virksomheter som etter § 3-3 er enheter i Kraftforsyningens beredskapsorganisasjon (KBO). Forskriften gjelder også for de virksomheter som etter vedtak blir KBO-enheter.
- § 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.



Kapittel 1. Innledende bestemmelser

— § 1-3. Hvem forskriften er rettet mot

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

— § 1-3. Hvem forskriften gjelder for

— 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.



Kapittel 1. Innledende bestemmelser

- § 1-3. *Hvem forskriften er rettet mot*
- Forskriftens § 6-2 om taushetsplikt for kraftsensitiv informasjon gjelder for enhver.
- § 1-3. *Hvem forskriften gjelder for*
- 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.
- Forskriftens § 6-2 om taushetsplikt for kraftsensitiv informasjon gjelder for enhver.



Oversikt over hva som gjelder for hvem (utdrag)

BESTEMMELSENE	KBO-enhet	Virksomheter med vedtak etter § 1-3 annet ledd	Virksomheter med vedtak etter § 1-3 tredje ledd	Enhver
§ 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			



KBF vd BFE

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 beredskapsplan		X	§ 2-3. Beredskapsplikt
§ 2-1 Kraftforsynings beredskapsorganisasjon		X	§ 3-1. Organisering av KBO og § 3-3. KBO-enheter
§ 2-2 Organisasjon og funksjon		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-enheter		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 kraftforsynings distriktssjefer
§ 3-5 Fritaksordninger		X	§ 3-7. Fritaksordninger
§ 3-6 Sektorvist responsmiljø for IKT-sikkerhetshendelser	X		NY

Kapittel 2.

Generelle krav for KBO-enheter



Kapittel 2. Generelle krav for KBO-enheter

- § 2-2. *Organisasjon og funksjon*
- Virksomhet som omfattes av denne forskrift skal ha følgende funksjoner:
 - a. *Beredskapsleder*. ~~Denne utpekes av leder for virksomheten~~ og skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet.

- § 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.



Kapittel 2. Generelle krav for KBO-enheter

- § 2-2. *Organisasjon og funksjon*

- b. *Beredskapskoordinator*. Denne skal være administrativt kontaktpunkt til beredskapsmyndigheten.
- c. *IKT-sikkerhetskoordinator*. Denne skal være faglig kontaktpunkt til beredskapsmyndigheten vedrørende IKT-sikkerhet.

- § 2-2. *Organisasjon og funksjon*

- 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.



Kapittel 2. Generelle krav for KBO-enheter

— § 2-6. Varsling og rapportering

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

— § 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. Varslet skal kortfattet beskrive hendelsen, forventet gjenoppretting og kontaktperson.



Kapittel 2. Generelle krav for KBO-enheter

§ 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, hæververk, 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.

§ 2-6- Rapportering

- 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.

Kapittel 3.

Kraftforsyningens beredskapsorganisasjon ~~(KBO)~~



Sårbarhetsvarsler og hendelseshåndtering

Rammeverk for håndtering av IKT-sikkerhetshendelser

Versjon per 07.12.17



KraftCERT



KraftCERT jobber for bedre sikring i prosesskontroll-systemer ved å bistå kraftbransjen slik at de skal være oppdatert om relevante sårbarheter og trusler, og at de skal være i stand til å detektere og motvirke digitale angrep.

KraftCERT bistår også i håndtering av digitale sikkerhetshendelser og er med i den nasjonale beredskapsorganisasjonen. KraftCERT jobber for en god, sikker og effektiv informasjonsdeling mellom relevante selskaper nasjonalt og internasjonalt.

Copyright © KraftCERT AS 2015.



Kapittel 3. Kraftforsyningens beredskapsorganisasjon

- ~~§ 3-6. Ansvar og oppgaver for kraftforsyningens distriktssjefer~~
- § 3-6. Sektorvist responsmiljø
- 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.



NVE

ENDRING AV BEREDSKAPSFORSKRIFTEN

I kraft fra 1.1.2019

Helge Ulsberg
Beredskapsseksjonen



Hele forskriften



Gjennomgående

- Alle KBO-enheter
- Kraftforsyningens distriktssjefer
- Sentralnett
- KBO-enheter
- KDS
- Transmisjonsnett

Kapittel 4.

Ressurser og reparasjonsberedskap



Endringer

— Ingen

— Ingen

Kapittel 5.

Klassifisering og sikringstiltak



Kapittel 5. Klassifisering og sikringstiltak (driftskontroll)

- § 5-1. *Sikringsplikt*
- Eier eller driver plikter å sikre ...
- § 5-2. *Klasser*
- Klasse I omfatter:
 - g. Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til d og f.
- § 5-1. *Sikringsplikt*
- Virksomheter plikter å sikre ...
- § 5-2. *Klasser*
- Klasse I omfatter:
 - h. Driftskontrollsystem som styrer eller overvåker anlegg som omfattet av bokstav a til g.



Kapittel 5. Klassifisering og sikringstiltak (driftskontroll)

- § 5-2. *Klasser*
 - Klasse 2 omfatter:
 - g. Driftskontrollsystem plassert i klasse 2 etter enkeltvedtak.
 - Klasse 3 omfatter:
 - e. Driftskontrollsystem plassert i klasse 3 etter enkeltvedtak.
- § 5-2. *Klasser*
 - Klasse 2 omfatter:
 - h. Driftskontrollsystem som styrer eller overvåker energiforsyningen til en befolkning på minst 50 000, eller flere anlegg omfattet av bokstav a til g.
 - Klasse 3 omfatter:
 - e. Driftskontrollsystem som styrer eller overvåker energiforsyningen til en befolkning på minst 250 000, eller flere anlegg omfattet av bokstav a til d.



Kapittel 5. Klassifisering og sikringstiltak (vannkraft)

- § 5-2. *Klasser*

- Klasse I omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 25 MVA.

- § 5-2. *Klasser*

- Klasse I omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 50 MVA.



Kapittel 5. Klassifisering og sikringstiltak (vindkraft)

- § 5-2. *Klasser*

- Klasse I omfatter:

- § 5-2. *Klasser*

- Nytt tredje ledd *Vindkraftanlegg klassifiseres ikke som kraftstasjon.*

- Klasse I omfatter:

- Ny bokstav g.

- g. Transformatorstasjon til vindkraftanlegg med samlet installert ytelse på minst 75 MVA. Dersom transformatorstasjonen også transformerer til nettførmål, klassifiseres den som transformatorstasjon etter bokstav b.



Kapittel 5. Klassifisering og sikringstiltak (vindkraft)

- § 5-2. *Klasser*

- Klasse 2 omfatter:

- § 5-2. *Klasser*

- Klasse 2 omfatter:

- Ny bokstav g.

- 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.



Kapittel 5. Klassifisering og sikringstiltak

— § 5-7. Vedtak om sikring eller klasse

- Beredskapsmyndigheten kan treffe vedtak om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av § 5-2 dersom det anses nødvendig.

Beredskapsmyndigheten kan treffe vedtak om at anlegg eller system skal klassifiseres i en annen klasse enn det som følger av tidligere vedtak dersom det anses nødvendig.

— § 5-7. Vedtak om sikring eller klasse

- Beredskapsmyndigheten 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.

Beredskapsmyndigheten kan treffe vedtak om at anlegg, system eller annet skal klassifiseres i en annen klasse enn det som følger av tidligere vedtak dersom det anses nødvendig.



Kapittel 5. Klassifisering og sikringstiltak

— § 5-8. *Analyse*

- Virksomhet som planlegger å bygge eller vesentlig endre eller utvide anlegg som er eller vil være klassifisert etter § 5-2, skal på bakgrunn av anleggets klasse etter § 5-2 eller enkeltvedtak, foreta en risiko- og sårbarhetsanalyse og prosjektere, utføre og sikre anlegg og system som angitt i denne forskrift.

— § 5-8. *Vurdering*

- Virksomheter som planlegger å bygge eller vesentlig endre eller utvide anlegg som er eller vil være klassifisert etter § 5-2, skal på bakgrunn av anleggets klasse etter § 5-2 eller enkeltvedtak, foreta en risikovurdering og prosjektere, utføre og sikre anlegg og system som angitt i denne forskrift.



Kapittel 5. Klassifisering og sikringstiltak

— § 5-9. Meldeplikt

- Virksomheter som planlegger å bygge, endre eller utvide konsesjonspliktige anlegg, skal senest ved søknad om konsesjon sende beredskapsmyndigheten skriftlig melding om hvilken klasse anlegget vil bli bygget etter, jf. § 5-2.
- For driftskontrollsystemer og annet uten konsesjonsplikt gjelder en tilsvarende plikt om melding i god tid før byggestart.

— § 5-9. Meldeplikt

- 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.



Kapittel 5. Klassifisering og sikringstiltak

- § 5-9. *Meldeplikt*
 - Melding skal gis elektronisk eller på annen måte som beredskapsmyndigheten bestemmer.
- § 5-9. *Meldeplikt*
 - Melding skal gis på den måten som beredskapsmyndigheten bestemmer.



Kapittel 5. Klassifisering og sikringstiltak

— § 5-10. Vakthold

- Eier eller driver av kraftforsyningsanlegg som er prioritert for vakthold i ekstraordinære situasjoner, skal bidra til planlegging og gjennomføring av vaktholdet i samarbeid med politi og forsvar.

— § 5-10. Vakthold

- Virksomheter som eier eller driver kraftforsyningsanlegg som er prioritert for vakthold i ekstraordinære situasjoner, skal bidra til planlegging og gjennomføring av vaktholdet i samarbeid med politi og forsvar.



Kapittel 5. Klassifisering og sikringstiltak

— § 5-11. Besøksrestriksjoner

- Alle driftssentraler i klassifiserte driftskontrollsystemer, og alle energianlegg klassifisert i klasse 3, skal ha besøksrestriksjoner.

Beredskapsmyndigheten kan vedta at også energianlegg i klasse 2 skal ha besøksrestriksjoner.

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

- Alle driftssentraler i klassifiserte driftskontrollsystemer, og alle energianlegg klassifisert i klasse 3, skal ha restriksjoner for adgang.

Beredskapsmyndigheten kan vedta at også energianlegg i klasse 2 skal ha restriksjoner for adgang.



Kapittel 5. Klassifisering og sikringstiltak

- § 5-11. Besøksrestriksjoner
- Ved anlegg underlagt besøksrestriksjoner skal:
 - c. Det ikke gis opplysninger om sensitiv informasjon etter § 6-2.
- § 5-11. Restriksjoner for adgang til steder og områder
- Ved anlegg underlagt restriksjoner for adgang skal:
 - ~~— c. Det ikke gis opplysninger om sensitiv informasjon etter § 6-2.~~



Kapittel 5. Klassifisering og sikringstiltak

- § 5-11. Besøksrestriksjoner
- Driftssentraler i klasse 3 skal ha besøksforbud.
- Beredskapsmyndigheten kan vedta besøksforbud for andre energianlegg i klasse 3.
- § 5-11. Restriksjoner for adgang til steder og områder
- 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 energianlegg i klasse 3.



NVE

ENDRING I BEREDSKAPSFORSKRIFTEN

I kraft 1.1.2019

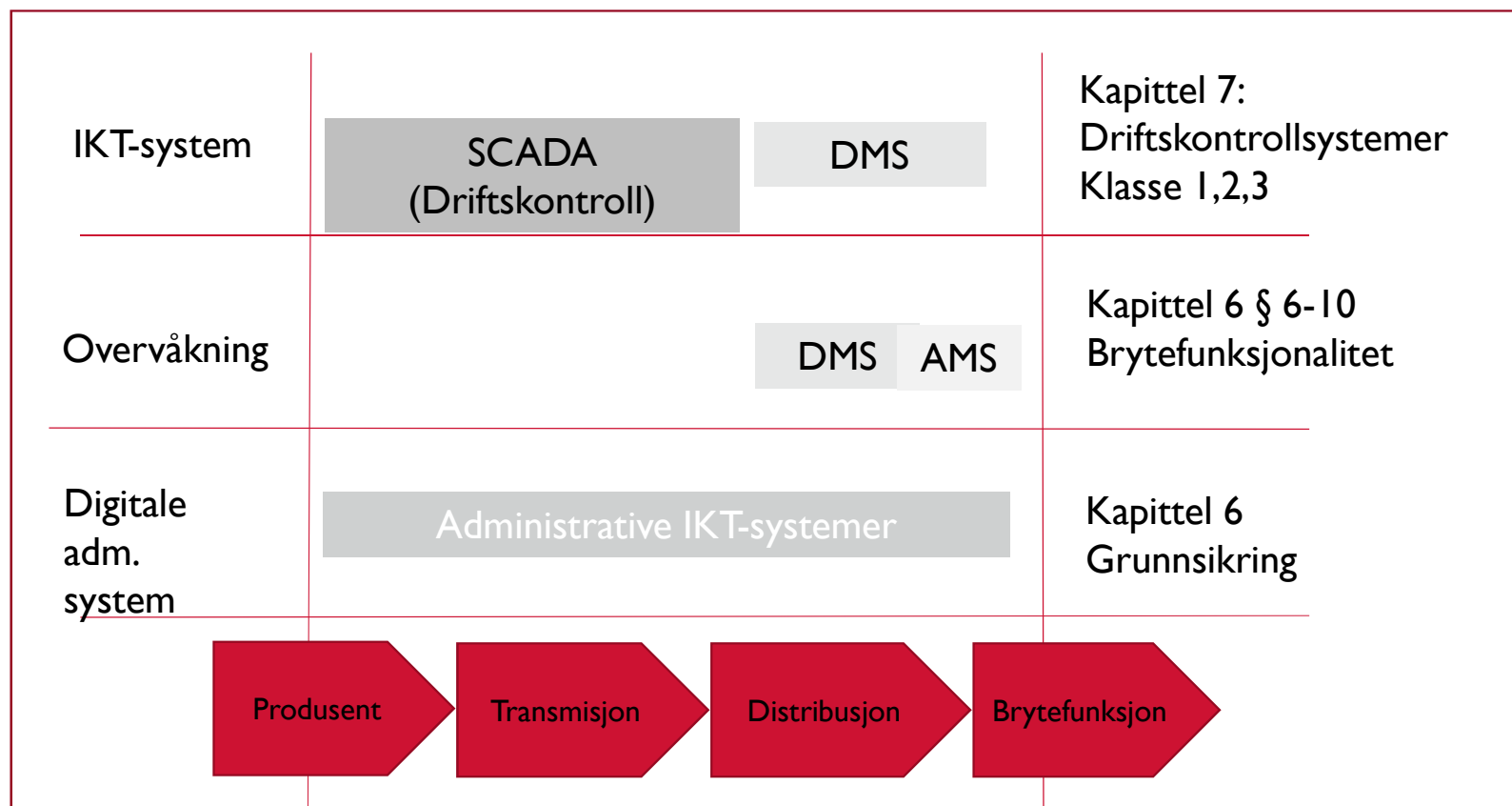
Janne Hagen
Beredskapsseksjonen



Kapittel 6

Informasjonssikkerhet

Helhetlig sikkerhet - rammeverk



Forsyningssikkerhet



Kraftsensitiv informasjon

- Plikten til å beskytte kraftsensitiv informasjon etter energiloven § 9-3 gjelder uavhengig av om en virksomhet underlegges beredskapsforskriften eller ikke.



Kapittel 6. Informasjonssikkerhet

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

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

§ 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.



Kapittel 6. Informasjonssikkerhet

Identifiseringen av hva som er sensitiv informasjon og hvor denne befinner seg, skal omfatte oppbevaring på papir, lagring i elektronisk form eller lagring på annen måte.

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.



Kapittel 6. Informasjonssikkerhet

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 innen sin virksomhet.



Kapittel 6. Informasjonssikkerhet

Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for sensitiv informasjon innenfor sin virksomhet og kan avgjøre om det er tjenstlig behov for å videreformidle sensitiv informasjon fra virksomheten til andre utenfor egen virksomhet. Beredskapsmyndigheten kan i tvilstilfeller avgjøre hvem som er rettmessig bruker.

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.



Kapittel 6. Informasjonssikkerhet

§ 6-2. *Sensitiv informasjon*

Med sensitiv informasjon menes spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen, herunder:

§ 6-2 Kraftsensitiv informasjon

Med kraftsensitiv informasjon menes spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen, herunder:....



Kapittel 6. Informasjonssikkerhet

§ 6-2 annet ledd, bokstav d:

Oversikt over fordelingsnett til samfunnskritiske funksjoner.

e. Nøyaktig kartfesting av jordkabler.

§ 6-2 annet ledd, bokstav d:

Oversikt over fordelingsnett og rørnett til samfunnskritiske funksjoner.

e. Nøyaktig kartfesting av jordkabler og rørnett til fjernvarmeanlegg med varmesentraler i klasse 2

÷



Kapittel 6. Informasjonssikkerhet

§ 6-2 annet ledd, bokstav d:

Oversikt over fordelingsnett til samfunnskritiske funksjoner.

e. Nøyaktig kartfesting av jordkabler.

g. Alle opplysninger om reservedriftssentraler og andre særskilte beredskapsanlegg for ledelse og drift, samt lokalisering av driftssentraler i klasse 2 og 3.

§ 6-2 annet ledd, bokstav d:

Oversikt over fordelingsnett og rørnett til samfunnskritiske funksjoner.

e. Nøyaktig kartfesting av jordkabler og rørnett til fjernvarmeanlegg med varmesentraler i klasse 2

g: Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift.



Kapittel 6. Informasjonssikkerhet

§ 6-3. Beskyttelse, avskjerming og tilgangskontroll

~~Alle KBO-enheter skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for sensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.~~

§ 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.



Kapittel 6. Informasjonssikkerhet

System og rutiner skal omfatte merking, oppbevaring, bruk og distribusjon, tilintetgjøring og tiltak for intern og ekstern rapportering av hendelser av betydning for informasjonssikkerheten.



Kapittel 6. Informasjonssikkerhet

Særskilte regler og sikkerhetstiltak skal utarbeides ved bruk av mobile enheter som kan motta, sende og lese sensitiv informasjon.



Kapittel 6. Informasjonssikkerhet

§ 6-4. Sikkerhetsinstruks

~~Alle KBO-enheter skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas, og som beskriver identifiseringen som er foretatt i henhold til § 6-1 og hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.~~

§ 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.



Kapittel 6. Informasjonssikkerhet

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.



Kapittel 6. Informasjonssikkerhet

§ 6-5. Anskaffelser i energiforsyningen

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



Kapittel 6. Informasjonssikkerhet

~~Det skal også i avtale opplyses at beredskapsmyndigheten kan føre tilsyn med etterlevelsen av disse bestemmelsene. Tilsvarende opplysningsplikt gjelder for leverandører når disse inngår kontrakt med underleverandører.~~



Kapittel 6. Informasjonssikkerhet

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



Begrenset anbudsinnbydelse

I § 6-6. Begrenset anbudsinnbydelse skal første ledd lyde.

Anbudsinnbydelser og lignende skal begrenses når det er nødvendig for å hindre at sikkerhetsgradert eller kraftsensitiv informasjon blir offentlig tilgjengelig gjennom anbudsdokumentene.



Krav til beskyttelse av kraftsensitiv informasjon

- § 6-3. Beskyttelse, avskjerming og tilgangskontroll skal lyde:
- 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



- § 6-4. Sikkerhetsinstruks skal lyde:
- *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.



Bakgrunnssjekk for personell

- § 6-7 endres ved at bruk av bakgrunnssjekk etter annet ledd gjøres betinget av KBO-enhetens egen risikovurdering.
- bruke andre egnede sikkerhetstiltak
- forslaget om politiattest vedtas på et senere tidspunkt



Ny § 6-7. Personkontroll



Kapittel 6 Informasjonssikkerhet

§ 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.



Ny § 6-9 Digitale informasjonssystemer



§ 6-9 Digitale informasjonssystemer

- Generell plikt
- Virksomheten har ansvar
- Grunnsikring



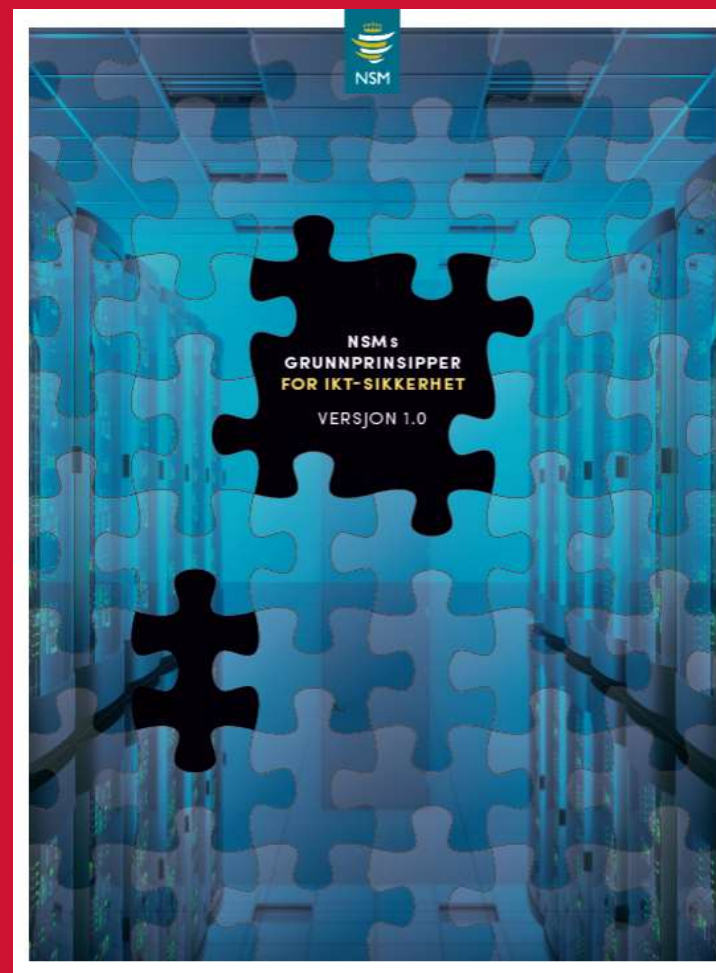
§ 6-9. *Digitale informasjonssystemer*

- Virksomheter plikter å 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.
- Virksomheten skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer, herunder:



§ 6-9 Digitale informasjonssystemer

- A) Identifisere og dokumentere
- B) Risikovurderinger





§ 6-9. *Digitale informasjonssystemer*

a) Identifisere og dokumentere

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

Dokumentasjonen skal *holdes oppdatert*.



§ 6-9. *Digitale informasjonssystemer*

b) Risikovurdering

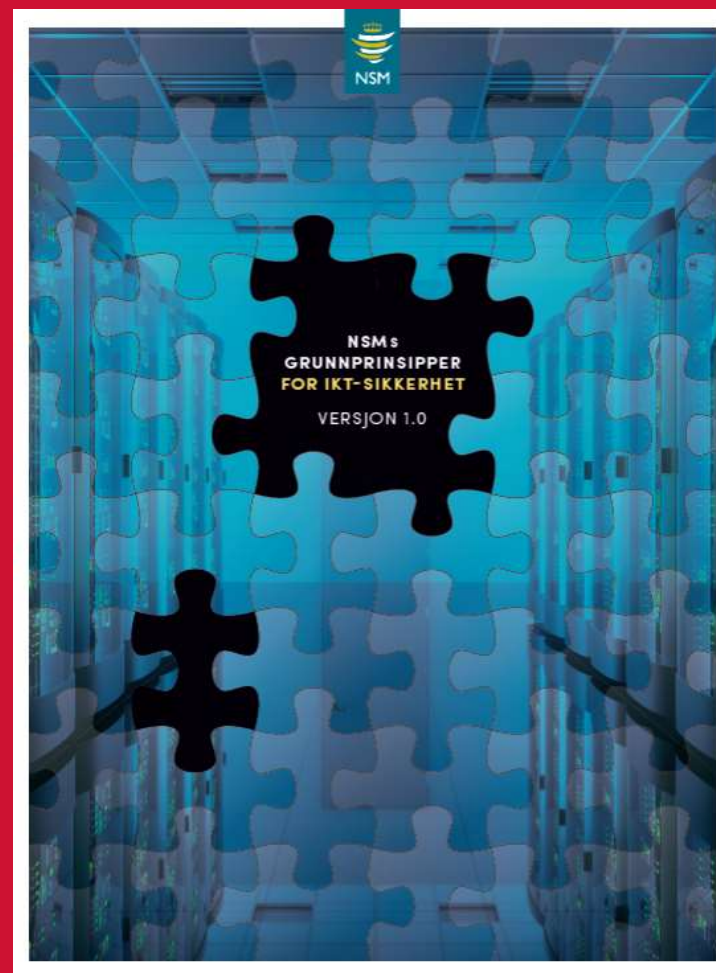
Virksomheten skal gjennomføres risikovurdering ved systemendringer.

Risikovurderingen skal holdes oppdatert.



§ 6-9 Digitale informasjonssystemer

- C) Sikre og oppdage
- D) Håndtere og gjenopprette





§ 6-9. *Digitale informasjonssystemer*

c) Sikre og oppdage

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

Virksomheten 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.



§ 6-9. Digitale informasjonssystemer

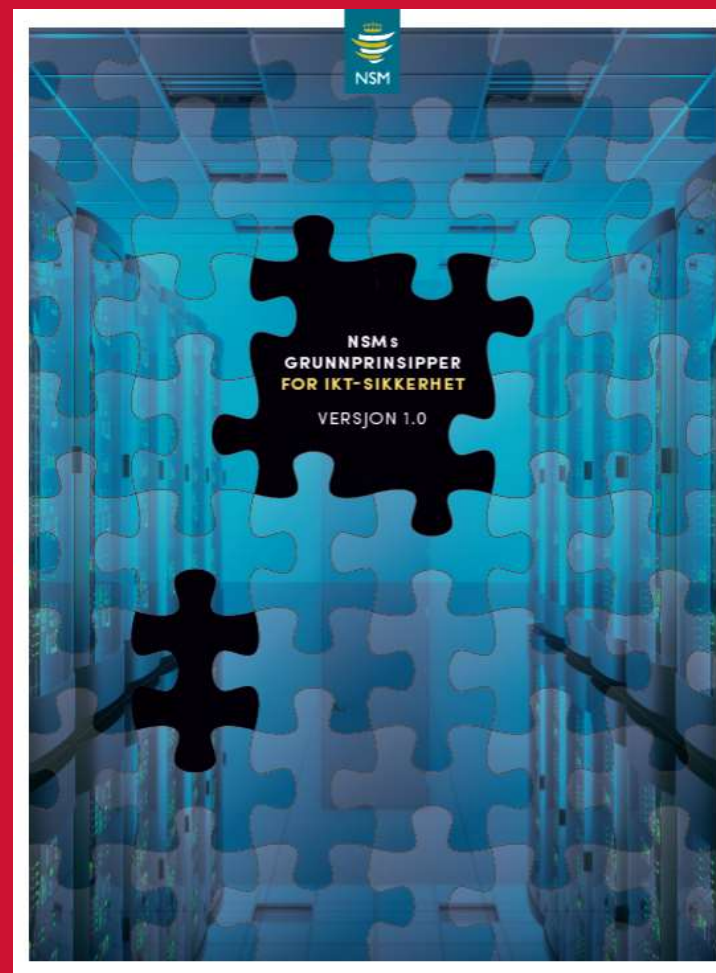
d) Håndtere og gjenopprette

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



§ 6-9 Digitale informasjonssystemer

- E) Tjenesteutsetting
- «Minst like god som i dag»





§ 6-9. *Digitale informasjonssystemer*

e) Tjenesteutsetting

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



§ 6-9 Digitale informasjonssystemer

- F) Sikkerhetsrevisjon



§ 6-9. Digitale informasjonssystemer

f) Sikkerhetsrevisjon

Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon av iverksatte beskyttelsestiltak i det digitale informasjonssystemet.

Revisjonen skal påse at tiltakene faktisk er etablert og fungerer etter sin hensikt.
Hver revisjon kan ta for seg deler av beskyttelsestiltakene.



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



Ny § 6-10. *Brytefunksjonalitet i avanserte måle- og styringssystem (AMS) skal lyde:*

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 netttjenester 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 brytefunksjonaliteten. 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 oppdateringsfunksjonen, som forhindrer at hendelser som kompromitterer sikkerheten i en måler, kompromitterer sikkerheten i en annen måler.



§ 8-3 er uendret

- § 8-3.*Dispensasjon*
- Beredskapsmyndigheten kan i særlige tilfeller gi dispensasjon fra bestemmelser gitt i eller i medhold av denne forskrift.



NVE

ENDRING AV BEREDSKAPSFORSKRIFTEN

I kraft fra 1.1.2019

Helge Ulsberg
Beredskapsseksjonen

Kapittel 7

Beskyttelse av driftskontrollsystem



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- Alle virksomheter med driftskontrollsystem skal sørge for at disse til enhver tid virker etter sin hensikt og skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser, ~~herunder mot alle typer uautorisert tilgang for å hindre misbruk og spredning av skadelig programvare og lignende.~~
- § 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.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- Nytt annet ledd:
- 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 driftskontrollsystemer.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- Nytt tredje og fjerde ledd:
- 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



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- Alle virksomheter med driftskontrollsystem er underlagt bestemmelsene om klassifisering og sikringsplikt etter kapittel 5.
- § 7-1. *Generell plikt til å beskytte driftskontrollsystemet*
- ~~— Alle virksomheter med driftskontrollsystem er underlagt bestemmelsene om klassifisering og sikringsplikt etter kapittel 5.~~



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-2. *Overordnede sikkerhetsregler*
- Virksomheten skal fastsette sikkerhetskrav for bruk, utvikling, drift, systemvedlikehold, sikring med mer av driftskontrollsystem slik at overvåking og kontroll av energiforsyningen kan utføres på en sikker måte.
- § 7-2. *Interne sikkerhetsregler*
- Virksomheter skal fastsette sikkerhetsregler for bruk, utvikling, drift, systemvedlikehold, sikring med mer av driftskontrollsystem slik at overvåking og kontroll av kraftforsyningen kan utføres på en sikker måte.

Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-2. Overordnede sikkerhetsregler
- Sikkerhetskravene skal gjennomgå minimum årlig for å klarlegge om de er hensiktsmessige i forhold til virksomhetens behov, om de etterleves, og om kravene gir tilfredsstillende beskyttelse av driftskontrollsystemet.
- § 7-2. Interne sikkerhetsregler
- Virksomheter skal gjennomgå sikkerhetsreglene minimum årlig for å sikre at de etterleves og at de gir tilfredsstillende beskyttelse.



Kapittel 7. Beskyttelse av driftskontrollsystem

— § 7-3. *Dokumentasjon av driftskontrollsystemet*

— § 7-3. *Dokumentasjon av driftskontrollsystemet*

— Ny setning i andre ledd:

— Dokumentasjonen skal også omfatte en komplett oversikt over utstyr i driftskontrollsystemet.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-4. *Kontroll med brukertilgang*
- Virksomheten skal ha kontrollordninger for tildeling, endring, sletting og vurdering av korrekt tilgang til driftskontrollsystemet.
- § 7-4. *Kontroll med brukertilgang*
- Virksomheter skal kontrollere at kun rettmessige brukere har tilgang til driftskontrollsystemet. For dette skal det være kontrollordninger for tildeling, endring og sletting av brukertilgang.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-4. *Kontroll med brukertilgang*
- Virksomheten skal til enhver tid kunne kontrollere hvilken person som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes.
- § 7-4. *Kontroll med brukertilgang*
- Virksomheter skal kontrollere hvilken bruker som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-5. *Kontroll ved endringer i driftskontrollsystemet*
- Virksomheten skal ha kontrollordninger for vurdering, testing og godkjenning av endringer i driftskontrollsystemet før disse utføres, for å hindre utilsiktede feil og påføring av nye sårbarheter.
- § 7-5. *Kontroll ved endringer i driftskontrollsystemet*
- Virksomheter skal hindre at utilsiktede feil og nye sårbarheter blir introdusert ved endring i driftskontrollsystemet. For dette skal det være kontrollordninger for vurdering, testing og godkjenning av endringer.

Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-6. *Kontroll med utstyr i driftskontrollsystemet*
- Utstyr som benyttes i driftskontrollsystemet tillates ikke brukt i andre nettverk eller løsninger utenom driftskontrollsystemet, heller ikke midlertidig.
- § 7-6. *Kontroll med utstyr i driftskontrollsystemet*
- Virksomheter skal sørge for at utstyr som benyttes i driftskontrollsystemet ikke har blitt brukt eller blir brukt utenom driftskontrollsystemet, heller ikke midlertidig.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-6. *Kontroll med utstyr i driftskontrollsystemet*
- Utstyr som benyttes for å etablere logiske eller fysiske skiller mellom prosessnettverk i driftskontrollsystemet og andre nettverk, skal ha effektive kontrollordninger som hindrer uautorisert tilgang mellom skillene.
- § 7-6. *Kontroll med utstyr i driftskontrollsystemet*
- Virksomheter skal hindre urettmessig tilgang mellom driftskontrollsystemet og andre informasjonssystemer.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-6. *Kontroll med utstyr i driftskontrollsystemet*
- Virksomheten skal ha en oppdatert oversikt over utstyr av vesentlig betydning for driftskontrollsystemets funksjon.
- § 7-6. *Kontroll med utstyr i driftskontrollsystemet*
- ~~— Virksomheten skal ha en oppdatert oversikt over utstyr av vesentlig betydning for driftskontrollsystemets funksjon.~~



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd
- Virksomheten skal etablere kontrollordninger for å sikre effektiv håndtering av feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemets funksjon.
- Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf. også § 2-6.
- § 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd
- Virksomheter skal håndtere feil, sårbarheter i programvare, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemet.
- Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf. §§ 2-5 og 2-6.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-10. *Ekstern tilkobling til driftskontrollsystemet*
- Virksomheten skal ha kontrollordninger for å godkjenne, vedlikeholde og avvikle ordninger for ekstern tilkobling til driftskontrollsystemet, samt funksjoner for innstilling av vern. En særskilt vurdering skal ligge til grunn for godkjenning av løsning.
- § 7-10. *Ekstern tilkobling til driftskontrollsystemet*
- Virksomheter skal ha kontroll med ekstern tilkobling til driftskontrollsystemet.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-10. *Ekstern tilkobling til driftskontrollsystemet*
- Kun autorisert personell kan gis adgang til driftskontrollsystemet gjennom ekstern tilgang. Virksomheten skal ha kontrollordninger for vurdering, tildeling, endring og tilbaketrekking av autorisasjon. Virksomheten skal ha en oppdatert liste over alle som er autorisert.
- § 7-10. *Ekstern tilkobling til driftskontrollsystemet*
- Kun godkjente brukere kan gis adgang til driftskontrollsystemet gjennom ekstern tilgang. Virksomheter skal ha en oppdatert liste over alle godkjente brukere.



Kapittel 7. Beskyttelse av driftskontrollsystem

~~— § 7-10. Ekstern tilkobling til driftskontrollsystemet~~

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

~~— For fjernvarmeanlegg der hele eller deler av driftskontrollfunksjonen utføres av selskap som ikke er KBO-enhet, må vedkommende KBO-enhet påse at hele driftskontrollsystemet beskyttes etter relevante bestemmelser i denne forskrift.~~

~~— § 7-10. Ekstern tilkobling til driftskontrollsystemet~~

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



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-11. Systemredundans i driftskontrollsystemet
 - Virksomheten skal vurdere behovet for redundans i driftskontrollsystemet basert på lokale forhold og risikoanalyse.
- § 7-11. Systemredundans i driftskontrollsystemet
 - Virksomheter skal vurdere behovet for redundans i driftskontrollsystemet basert på lokale forhold og risikovurdering.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-12. *Sammenkobling mellom avanserte måle- og styringssystem (AMS) og driftskontrollsystem*
- ~~Dersom virksomheten har integrert funksjonalitet for bryting og begrensnings av effektuttak i avanserte måle- og styringssystem (AMS), jf. forskrift om måling, avregning og samordnet opptreden ved kraftomsetning og fakturering av nettenester § 4-2 e, i virksomhetens driftskontrollsystem, skal IKT-system med tilhørende utstyr som benyttes til denne funksjonen, sikres i henhold til driftskontrollsystemets klasse.~~
- ~~Med integrert funksjonalitet menes at funksjonen for å bryte og begrense effekt ved AMS utøves fra virksomhetens driftssentral, og at man benytter samme utstyr og infrastruktur som virksomheten benytter i driftskontrollsystemet.~~
- ~~Bestemmelsen gjelder til og med det utstyr eller punkt der signalene for å bryte og begrense effektuttak adskilles fra signalene i driftskontrollsystemet.~~
- § 7-12. *Integrasjoner mellom driftskontrollsystem og andre informasjonssystemer*
- Oppheves.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-14. Særskilte krav til driftskontrollsystem klasse 2
 - f. Ekstern tilkobling til driftskontrollsystemet
 - Virksomheten skal ha kontrollordning for korrekt autentisering av de personene som er autorisert til å benytte ekstern tilkobling for adgang til driftskontrollsystemet.
- § 7-14. Særskilte krav til driftskontrollsystem klasse 2
 - f. Ekstern tilkobling til driftskontrollsystemet
 - 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.



Kapittel 7. Beskyttelse av driftskontrollsystem

- § 7-14. Særskilte krav til driftskontrollsystem klasse 2
- Ny bokstav k
- § 7-14. Særskilte krav til driftskontrollsystem klasse 2
- k. Krav til leverandører
- For leveranser til driftskontrollsystemet tillates kun utenlandske leverandører fra et land som er medlem i EFTA, EU eller NATO. En leveranse omfatter levering av utstyr, komponenter, programvare, data, programmeringstjenester, oppdateringer, feilretting, service og vedlikehold.



NVE

ENDRING AV KRAFTRASJONERINGSFORSKRIFTEN

Innlemming av krav til rasjoneringsplaner i forskrifta

Synnøve Lill Paulen
Senioringeniør, seksjon for kraftsystem



Oppdatering av regelverket for kraftrasjoning

- Høring med forslag om innlemming av krav i forskriftstekst
- Frist for innspel 20. mai
- Det kom 17 innspel til høringa
- Endelig forskriftstekst er justert på enkelte punkt etter innspel
- Fleire innspel på rettleiar
- Innspel til nye vurderingar for utvida bruk av AMS
- Ny forskriftstekst vedtatt 1.11.2018 – trer i kraft 1.1.2019
- Oppdatert rettleiar vil bli publisert i desember



Nytt §6a om rasjoneringsplaner

Alle virksomheter som er KBO-enheter etter kraftberedskapsforskriften § 2-1 og som har områdekonsesjon etter energiloven § 3-2, plikter å utarbeide rasjoneringsplaner som en del av sin beredskapsplanlegging. Dette gjelder ikke virksomheter som kun leverer kraft til eget forbruk.

Virksomheter omfattet av første ledd, skal utarbeide rasjoneringsplaner med utgangspunkt i ansvarsområdet til den enkelte KBO-enhet og anlegg omfattet av områdekonsesjonsordningen. Rasjoneringsplanen skal inneholde alle elementer som fastsatt i vedlegg 1.

Rasjoneringsplaner skal koordineres med andre relevante KBO-enheter og KDS etter kraftberedskapsforskriften § 2-1 i det aktuelle området.



Utdjuping av krav til element som skal med i planen

- Organisering og informasjonshåndtering
- Samarbeid med andre aktører og prioritering av sluttbrukarar
- Utkobling av uprioritert
- Kvoterasjonering
- Sonevis roterande utkoblinger



Mulig framtidig bruk av AMS i kvoterasjonering

- AMS kan legge til rette for at kvoter blir overholdt
 - Ikkje lenger krav til egenmelding av forbruk og kontrollar av dette
- Mulig utvida bruke av AMS
 - Utkobling dersom kvota brukast opp som alternativ til overforbrukstariff?
 - Mulig mellomsteg mellom kvoterasjonering og sonevis roterande utkobling?
 - Kan føre til auka kostnadar for selskapa på grunn av planlegging og andre krav til funksjonalitet samtidig som at sikkerhet må ivaretas
- NVE fikk fleire innspel på dette – desse tar vi med i den vidare vurderinga



SPØRSMÅL?

sylp@nve.no