

Veiledning til forskrift om sikkerhet og beredskap i kraftforsyningen (Kraftberedskapsforskriften)



(Foto: Statnett)

Dette dokumentet inneholder veiledning til kraftberedskapsforskriftens kapittel 1-8, inklusive vedlegg til kapittel 5.

Maler og skjemaer er å finne på www.nve.no.

All dokumentasjon gjengitt her er tilgjengelige på www.nve.no.

Endringslogg Kbf 15.12.2022, versjon 1.3

NVE har oppdatert veiledningen. Endringer framgår av tabellen under. NVE takker spesielt NEK for deres gjennomgang av veilederen og innspill til bruk av standarder.

Kapittel	Endring
1	I avsnitt 1-3, tabelloversikt: § 5-1 sikringsplikten kan også gjelde virksomheter med vedtak etter § 1-3.
2	«Skal»-listen til virksomhetsleder er utvidet. Nye standarder er lagt til Generell språkvask og fjerning av utdatert informasjon
3	Endret illustrasjon: Organisering av KBO s. 2 og 3. Figur A er ny. Figur B er uendret § 3-5 peker til lovverk som ikke lenger er gjeldende (politireserven) Midlertidig fritak fra tjeneste for tjenesteppliktige i sivilforsvaret er nå endret til forskrift om sivilforsvar. Generell språkvask og fjerning av utdatert informasjon
4	Innholdet er uendret, mindre tekstlige endringer.
5	Uendret
6	Underkapittel 6.7 har ny veiledningstekst med nedtoning av bruk av kredittvurdering og større vekt på risikovurdering, bruk av andre sikringstiltak rettet mot innsidetrusler og vektlegging av god personalledelse gjennom hele ansettelsesperioden. Tiltakene gjelder hele perioden. Endringen skyldes at kravet til kredittvurdering er i konflikt med personopplysningsforskriften § 4-3. Kapittel 6.9 peker på minimumsnivå til å gjelde kategori 1 og 2 grunnprinsipper – det utgjør totalt 35 tiltak. Kapittel 6-10 henviser til ny veileder fra RME – veileder til sikkerhet i AMS. Øvrige endringer og korreksjoner omfatter kontroll av internett-lenker og mindre språklige korreksjoner.
7	Underkapittel 7-1 har henvisning til NEK-standarder som ikke var henvist til i forrige versjon. Mindre språklige rettinger.
8	Uendret
Maler	Maler og skjema er uendret.

Innhold

Kraftberedskapsforskriften (kbf)	1
1. Innledende bestemmelser	2
1.1 Formål	2
1.2 Virkeområde	3
1.3 Hvem forskriften gjelder for	4
1.4 Ansvar	6
1.5 Beredskapsplikt og beredskapsplan	7

Kraftberedskapsforskriften (kbf)

Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften) FOR-2012-12-07-1157, Kraftberedskapsforskriften (kbf), er hjemlet i Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) av 29. juni 1990 nr. 50, kapittel 9 om beredskap. Virksomheter og personell som faller innenfor energilovens og kraftberedskapsforskriftens virkeområde, plikter å oppfylle kravene som gjelder i både energiloven kapittel 9 og kraftberedskapsforskriften.

Veilederen til kraftberedskapsforskriften forklarer mer detaljert hvem som er omfattet av forskriften, og viser gjennom eksempler hvordan kravene i forskriften kan oppfylles. Å velge metoder som angitt i veilederen vil anses som godt nok til å oppfylle forskriftens krav. Der forskriften oppstiller funksjonskrav, kan virksomhetene velge andre like gode løsninger og metoder.

Veilederen er bygget opp på følgende måte:

- Kapitler: Veilederen er inndelt i samme kapitler som forskriften. Hvert kapittel starter med en kort introduksjon til kapitlet.
- Forskriftens kapitler inneholder krav i form av paragrafer. Veilederen gjengir forskriftsteksten til hver paragraf, en kort forklaring av kravene i paragrafen om nødvendig, ordforklaring og veiledning til hvordan kravene kan oppfylles i praksis. NVEs forklaring av kravene er illustrert i eksempler der det er relevant. Eksempelene bygger på spørsmål fra bransjen om forskriften og NVEs svar. NVE har valgt å benytte fiktive navn på virksomheter i eksemplene.
- I veilederen henviser NVE videre til andre veiledere, for eksempel NSMs veiledere på sikkerhet eller REN blad, temarapporter utarbeidet av NVE eller andre myndigheter og organisasjoner. Veilederen henviser videre til maler og skjema fra NVE og nasjonale og internasjonale standarder. NVE anbefaler at brukere av veilederen henter mer kunnskap og råd i disse refererte dokumentene når virksomheten ser det er relevant. Merk at NVE fører tilsyn med etterlevelsen av forskriftskravene, ikke med etterlevelse av denne veilederen, standarder og andre temadokumenter det er henvist til i denne veilederen.

- Avslutningsvis til hver bestemmelse viser veilederen krysskoblinger til andre paragrafer i forskriften eller til andre forskrifter der det er relevant.

Bruk av symboler:

Krav	Eksempel	Sjekkliste	Obs!	Mer info
				

1. Innledende bestemmelser

Kapittel 1 presiserer formålet med kraftberedskapsforskriften, virkeområdet og hvem som er omfattet av forskriften. Beredskap i kraftforsyningen er i tillegg til beredskapskapitlet i energiloven og kraftberedskapsforskriften, regulert i energilovforskriften § 3-5 bokstav c og i § 5-3 bokstav c. Pliktene her gjelder alle som har konsesjon for elektriske anlegg (§3-5 c) eller konsesjon for fjernvarmeanlegg (§5-3 c). Konsesjonærer som ikke er KBO-enheter, kan finne råd om beredskapsarbeidet i veiledningen til kraftberedskapsforskriften og i [Fjernvarmeberedskap, veiledning 2015](#). Kapittel 1 peker videre til resten av kraftberedskapsforskriften

1.1 Formål

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

Ordforklaring

Opprettholde	Holde gående; holde ved like; bevare
Ekstraordinære situasjoner	Ekstraordinær: Som (ytterst) sjelden er tilfellet eller finner sted; usedvanlig; merkelig; ualminnelig En ekstraordinær situasjon påfører kraftforsyningen oppgaver som utfordrer normal ressursbruk og driftspraksis og påkaller ekstra innsats. En ordinær driftsforstyrrelse som ikke rettes, kan over tid gå over til å utgjøre en ekstraordinær situasjon
Effektiv	Måloppnåelse med riktig og tilstrekkelig ressursbruk

Kraftberedskapsforskriftens formål ligger innenfor Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energilovent) av 29. juni 1990 nr. 50, energilovens (enl.), formålsbestemmelse. Formålet med energilovent er å "sikre at produksjon, omforming, overføring, omsetning, fordeling og bruk av energi foregår på en samfunnsmessig rasjonell måte, herunder skal det tas hensyn til allmenne og private interesser som blir berørt", jf. enl. § 1-2.



Standarder

[NS-EN-ISO 22300:2018 Sikkerhet og resiliens - Terminologi \(ISO 22300:2018\)](#)

[NS-ISO 22320:2018 Sikkerhet og resiliens - Kriseledelse - Retningslinjer for hendelseshåndtering](#)

[NS-ISO 22326:2018 Sikkerhet og resiliens - Kriseledelse - Retningslinjer for overvåking av anlegg med identifiserte farer](#)

[SN-ISO/TS 22330:2018 Sikkerhet og resiliens - Ledelsessystemer for forretningskontinuitet - Retningslinjer for omsorgsbevisst forretningskontinuitet](#)

1.2 Virkeområde



§ 1-2. Virkeområde

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

Ordforklaring

Ekstraordinære situasjoner	Se § 1-1
-----------------------------------	----------

Kravene i kraftberedskapsforskriften pålegger virksomheten plikter som må oppfylles mens virksomheten er i normal driftsituasjon og før det er oppstått en ekstraordinær situasjon. Pliktene kan ivaretas ved å iverksette forebyggende sikringstiltak og planlegge og forberede beredskapstiltak.

Kravene i kraftberedskapsforskriften pålegger virksomheten plikter i og etter alle former for ekstraordinære situasjoner som kan skade eller hindre kraftforsyningen.

Krysskoplinger til annet regelverk

[Forskrift om leveringskvalitet i kraftsystemet](#)

[Forskrift om systemansvaret i kraftsystemet](#)

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 anvendes.

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.

Kraftberedskapsforskriften § 1-3 kort oppsummert:

Type virksomhet	Relevante krav
Virksomheter som eier eller driver klassifiserte anlegg er KBO-enheter	Hele kraftberedskapsforskriften gjelder
Andre virksomheter som er KBO-enhet etter særskilt vedtak i NVE	Her framgår det av vedtaksbrevet hvilke krav i kbf som gjelder for virksomheten
Virksomheter som er underlagt kbf som har fått innvilget dispensasjon fra forskriftens krav gjennom enkeltvedtak	Her framgår det av vedtaksbrevet hvilke krav som er unntatt for virksomheten
Enhver	<i>Alle</i> som får tilgang eller kjennskap til kraftsensitiv informasjon, både fysiske og juridiske personer.

Krysskopling til annet regelverk

[Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.](#)

[\(energilovforskriften\)](#) §§ 3-5a Drift, vedlikehold og modernisering og 5-3 a Drift og vedlikehold og §§ 3-5c og 5-3 c Beredskap.

BESTEMMELSENE	KBO-enhet	Virksomheter med vedtak etter §1-3		Enhver
		annet ledd	tredje ledd	
§ 1-4. Ansvar	x	x		
§ 1-5. Beredskapsplikt og beredskapsplan	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. Reparasjonsberedskap	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		

BESTEMMELSENE	KBO-enhet	Virksomheter med vedtak etter §1-3		Enhver
		annet ledd	tredje ledd	
§ 7-3. Dokumentasjon av driftskontrollsystemet	x	x		
§ 7-4. Kontroll med brukertilgang	x	x		
§ 7-5. Kontroll ved endringer i driftskontrollsystemet	x	x		
§ 7-6. Kontroll med utstyr i driftskontrollsystemet	x	x		
§ 7-7. Håndtering 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. Særskilte 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	x	
§ 8-2. Pålegg (vedtakshjemmel)	x	x	x	
§ 8-3. Dispensasjon (vedtakshjemmel)	x	x	x	
§ 8-4. Tvangsmulkt (vedtakshjemmel)	x	x	x	
§ 8-5. Overtredelsesgebyr (vedtakshjemmel)	x	x	x	
§ 8-6. Straff (vedtakshjemmel)	x	x	x	
§ 8-7. Gebyr til beredskapsmyndigheten	x			
§ 8-8. Forholdet til eldre vedtak om klassifisering og overgangsregler	x	x	x	

1.4 Ansvar

§

§ 1-4. Ansvar

Leder for virksomhet som er omfattet av denne forskrift har ansvar for at virksomheten er organisert og har funksjoner og ressurser slik at virksomheten er innrettet for å oppfylle kravene i energiloven kapittel 9, energilovforskriften § 3-5 bokstav c, § 5-3 bokstav c, og at bestemmelser gitt i eller i medhold av denne forskrift oppfylles.

Virksomhetens leder må kjenne til innholdet i energilovens kapittel 9 og kraftberedskapsforskriften, samt krav i energilovforskriften om beredskap.

Leder for virksomheten kan være både daglig leder, styreleder, hele styret og/eller resten av toppledelsen. Hvem som skal regnes som leder i virksomheten, må være tydelig angitt av virksomheten. Det er virksomheten selv som er ansvarlig for dette. Ansvarer innebærer å organisere virksomheten slik at kravene til funksjoner og ressurser oppfylles.

1.5 Beredskapsplikt og beredskapsplan



§ 1-5. Beredskapsplikt og beredskapsplan

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

Virksomheter som er omfattet av denne forskrift skal ha en beredskapsplan for å håndtere og begrense virkningene av ekstraordinære situasjoner.

Virksomhetene oppfyller kravet ved å følge kraftberedskapsforskriftens krav.

For KBO-enheter er kravene til beredskap ytterligere beskrevet i kbf kapittel 2, 3 og 4.

Kravet om effektiv sikring oppfyller virksomheten ved å følge kravene i kbf kapittel 5, 6 og 7.

Se standarder til § 1-1.



Innhold

2. Generelle krav for KBO-enheter	1
2.1 Kraftforsyningens beredskapsorganisasjon	1
2.2 Organisasjon og funksjon	2
2.3 Risikovurdering	6
2.4 Beredskapsplanlegging	8
2.5 Varsling	10
2.6 Rapportering	12
2.7 Øvelser	15
2.8 Informasjonsberedskap	17
2.9 Evaluering	18
2.10 Internkontrollsystem	20

2. Generelle krav for KBO-enheter

I kapittel 2 er det KBO-enhetenes oppgaver og funksjon som blir beskrevet. Kapittelet gir en fullstendig oversikt over de generelle kravene som stilles til hver enkelt virksomhet som regnes som en KBO-enhet, uansett om de har klassifiserte anlegg eller blitt oppnevnt gjennom enkeltvedtak. De ulike paragrafene retter seg mot hva den enkelte virksomhet må ha på plass av roller og funksjoner i tillegg til hvilke oppgaver som virksomheten har ansvar for at blir utført.

2.1 Kraftforsyningens beredskapsorganisasjon

§

§ 2-1. Kraftforsyningens beredskapsorganisasjon

Med KBO menes kraftforsyningens beredskapsorganisasjon. KBO består av KBO-enhetene, KDS og beredskapsmyndigheten, samt KSL, når denne trer i kraft, jf. § 3-3.

Med KBO-enhet menes:

- De virksomheter som eier eller driver anlegg, system eller annet og som i medhold av § 5-2 eller § 5-7 er klassifisert etter denne forskrift*
- Andre virksomheter beredskapsmyndigheten har vedtatt er KBO-enhet i medhold av § 3-1 annet ledd*

Med KDS menes kraftforsyningens distriktssjefer.

Med KSL menes kraftforsyningens sentrale ledelse. Kraftforsyningens sentrale ledelse består av beredskapsmyndigheten med deltakelse fra Statnett SF.

Bestemmelsen er ment å gi en oversikt over de ulike delene kraftforsyningens beredskapsorganisasjon er inndelt i.

KBO-enheter er større kraftprodusenter, nettselskaper, fjernvarmeselskaper og større vindkraftverk som har klassifiserte anlegg, jf. kap. 5 i denne forskriften. I tillegg er enkelte andre virksomheter av vesentlig betydning for kraftforsyningen også utpekt av NVE som KBO-enheter. Virksomheter som ikke har klassifiserte anlegg, må være utpekt av NVE gjennom enkeltvedtak (jf. § 3-1) om de skal være KBO-enheter. Virksomheter som ikke har klassifiserte anlegg, men som er viktige lokalt (f.eks. forsyner kritisk infrastruktur), kan be NVE om å bli utpekt som KBO-enhet.

Ytterligere informasjon om KBO som organisasjon, KDS og KSL er nærmere beskrevet i kapittel 3 i denne forskrift.

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*

Kravet til organisasjon og funksjon er satt for å sikre at det blir utpekt personer som er ansatt i virksomheten eller i konsernet, og som gis et spesielt ansvar for at kravene i forskriften etterleves. Personene skal også være kjente kontaktpunkt for NVE, slik at dialog om beredskap og sikkerhet på vegne av virksomheten er mulig. NVE betrakter funksjonene beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator som en del av virksomhetens kjernevirksomhet innenfor området beredskap. Funksjonene kan altså ikke tjenestestettes eller deles mellom ulike virksomheter. Et unntak er i konsern der NVE har tillatt at konsernet innehar funksjonene beskrevet i § 2-2 på vegne av datterselskapene.

Formålet med å utpeke funksjonene er at KBO-enheten skal utvikle og bevare viktig kompetanse og kapasitet til å håndtere uønskede situasjoner, ulykker, skader og andre *ekstraordinære situasjoner* som utgjør en *fare* eller *trussel* for viktige anlegg og systemer. KBO-enhetene må ta hensyn til at kritisk viktige medarbeidere kan være forhindret fra å stille opp i en ekstraordinær situasjon og at en pågående situasjon kan vare over tid. Det må være utpekt stedfortredere som kan fylle de nevnte funksjonene slik at de alltid er operative. Når det ikke er tillatt å for eksempel dele IKT-sikkerhetsrollen mellom ulike virksomheter, så handler det også om at IKT-sikkerhetskoordinatoren ikke skal bli satt i en interessekonflikt mellom flere virksomheter. Effektiv beredskap krever klare ansvarslinjer. Dette kommer i tillegg til kravene i energilovforskriften § 3-6 om tilgang til personell.

KBO-enhetene er selv ansvarlig for å holde NVE oppdatert om hvem som har de ulike funksjonene. Informasjon om funksjoner må oppdateres fortløpende inn i en felles digital løsning i Altinn. Om KBO-enheten skifter eller oppretter nytt organisasjonsnummer ved f.eks. konsesjonsoverdragelse, så må dette opplyses om særskilt til NVE sitt postmottak. Beredskapsseksjonen i NVE behandler denne informasjonen, så sett gjerne seksjonssjef i beredskapsseksjonen på kopi. Kontaktinformasjon finnes på NVE sine nettsider. Oppdatert informasjon om KBO-enhetene er viktig for at NVE til enhver tid skal kunne ha god oversikt over kontaktpunkter i hele KBO.

Etter § 1-4 er det virksomhetens leder som er ansvarlig for at kravene i § 2-2 oppfylles. Dette betyr at:

Virksomhetsleder *skal*:

- utpeke beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator i sin virksomhet
- være ansvarlig for at NVE blir holdt løpende oppdatert om hvem som til enhver tid fyller de ulike funksjonene
- være ansvarlig for at henvendelser og vedtak fattet av NVE blir fulgt opp av virksomheten, (jf. § 1-4)
- utpeke nødvendige stedfortredere

Virksomhetsleder *bør* i tillegg:

- kjenne til kravene i energiloven, energilovforskriften og kraftberedskapsforskriften
- sørge for at ansatte har kompetanse i hvordan kravene skal forstås og håndteres
- sørge for at beredskapsfunksjonene har eller får tilført kompetanse

Beredskapsleder *skal*:

- kunne dokumentere at planene for beredskapsarbeidet er dimensjonert for virksomhetens ansvarsområde
- kunne dokumentere utøvelsen av beredskapsarbeidet
- ha god oversikt over virksomhetens beredskapsorganisasjon

Beredskapsleder *bør* i tillegg:

- ha kjennskap til forebyggende sikkerhet og beredskap i kraftforsyningen, inkludert kravene i kraftberedskapsforskriften
- ha kjennskap til kraftforsyningen og om tilgrensende KBO-enheter
- ha oversikt over samfunnsviktige funksjoner i eget område

Beredskapskoordinator *skal*:

- være virksomhetens administrative kontaktpunkt mot NVE for alle henvendelser utenom IKT-relaterte utfordringer
- koordinere formidling av informasjon, henvendelser og vedtak fra NVE internt i virksomheten

- ha god oversikt over hvordan beredskapsarbeidet i virksomheten utøves i praksis
- koordinere planlegging, gjennomføring og oppfølging av virksomhetens beredskapsarbeid og ha oversikt over samfunnsviktige funksjoner i eget område
- bidra til at henvendelser fra NVE blir fulgt opp av virksomheten

Beredskapskoordinator bør i tillegg:

- ha inngående kunnskap om gjeldende lover og forskrifter innenfor forebyggende og konsekvensreduserende sikkerhet og beredskap i kraftforsyningen, inkludert kravene i kraftberedskapsforskriften
- ha god oversikt over interne krav til virksomhetens sikkerhets- og beredskapsarbeid
- god kjennskap til risiko- og sårbarhetsvurderinger, samt relevante farer og trusler mot sin virksomhet

IKT-sikkerhetskoordinator skal:

- være virksomhetens faglige kontaktpunkt mot NVE for IKT-relaterte utfordringer
- koordinere formidling av informasjon, henvendelser og vedtak fra NVE med betydning for IKT-sikkerhet internt i virksomheten
- ha god oversikt over interne krav til KBO-enhetenes IKT-sikkerhets- og beredskapsarbeid
- koordinere planlegging, gjennomføring og oppfølging av virksomhetens arbeid med beskyttelse av driftskontrollsystem, og virksomhetens øvrige IKT-system som inneholder kraftsensitiv informasjon eller informasjon av betydning for virksomhetens ledelse eller drift
- bidra til at henvendelser fra NVE om IKT-sikkerhetstema blir fulgt opp av virksomheten

IKT-sikkerhetskoordinator bør i tillegg:

- ha inngående kunnskap om gjeldende lover og forskrifter innenfor IKT-sikkerhet og beredskap i kraftforsyningen, inkludert kravene i kraftberedskapsforskriften
- ha god kunnskap om virksomhetens driftskontrollfunksjoner og administrative datasystemer, deres funksjonalitet, og hvordan de skal beskyttes
- ha god kjennskap til IKT-trusselbildet
- ha dialog eller informere KraftCERT om IKT-forhold som er utfordrende for KBO-enheten, eller forhold som kan være av interesse for KraftCERT sin IKT-oversikt over kraftsektoren



Om innrapportering av kontaktinformasjon i Altinn

Leder av virksomheten har ansvar for å innrapportere kontaktinformasjon ved organisasjons-, personal eller andre viktige kontaktinformasjonsendringer så raskt som mulig i Altinn. Se NVE sine hjemmesider for mer informasjon.

<https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/innrapportering-av-kontaktinformasjon-for-kbo-enheter/>

Om IKT-sikkerhetskoordinator og beredskapskoordinator i små virksomheter

I små virksomheter kan det være tilstrekkelig at en og samme person har ulike funksjoner. Forskriften gir ikke krav om at hver av funksjonene utgjør 100 % stillinger. Det viktigste er at virksomheten fyller funksjonen på en god måte.



Om plassering av forskriftsfestede roller i KBO

Roller skal som hovedregel legges til KBO-enhetene, *ikke* konsern. Konsernet er svært sjeldent KBO-enhet. Det å legge slike roller til konsernet gir økt avstand til de daglige utfordringene og kan resultere i lengre responstid der tid er essensiell. Konsernet kan ha flere datterselskap som er KBO-enheter. Det kan gi prioriteringskonflikter for de som innehar rollene om to eller flere av KBO-enhetene er berørt. Komplekse konsernstrukturer kan hindre god rolleforståelse for kjerneoppgavene den enkelte KBO-enhet har. NVE ser det som svært viktig at våre kontaktpunkter mot KBO-enheten har god rolleforståelse og god innsikt i virksomheten vedkommende representerer. Vi anbefaler derfor at rollene innehas av virksomheten som (eier og) driver i henhold til konsesjon eller områdekonsesjon.

Både pandemier, sikkerhetspolitiske eller andre langvarige situasjoner eller hendelser krever personell med god rolleforståelse og tilstrekkelig innsikt i sin virksomhet.



Vedtak

Vedtak om beredskapsmessig kommunikasjonsmidler i KBO av 16.12.2015. Unntatt offentlighet jf. Offl. § 21

Krysskopling til annet regelverk

[Energilovforskriften § 3-6 Tilgang til personell](#)

2.3 Risikovurdering



§ 2-3. Risikovurdering

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

Formålet med å gjennomføre risikovurderinger er å skaffe virksomheten et faglig grunnlag for å identifisere og håndtere risiko som virksomheten er utsatt for. Gjennom risikoanalysen kan virksomheten identifisere farer og trusler, samt sårbarheter, og identifisere preventive tiltak som må iverksettes for å få ned risikoen til et akseptabelt nivå. Merk da at § 5-3 i denne forskrift stiller krav til at risikoen blir minst mulig. *Akseptabelt nivå* regnes da som *minst mulig*. Risikovurderingene bør inkludere gjennomførte tiltak og justere restrisiko i forbindelse med gjennomgangen. Videre skal konsekvensreducerende tiltak beskrives nærmere i beredskapsplanen for den restrisikoen som aksepteres. Vurderingene må minst gjennomgås årlig fordi omverdenen er i stadig endring. Risikovurderingene skal brukes som systematiske prosessverktøy, spesielt når det har skjedd vesentlige endringer på menneskelig, teknologisk eller organisatorisk nivå.

Risikovurderingene må være av et slikt omfang at de gir en tilstrekkelig oversikt over risiko både på et overordnet og et mer detaljert nivå. Vedlegg 1 i NVEs veileder i risiko- og sårbarhetsanalyser gir en ikke-uttømmende liste over anlegg og funksjoner som minimum bør vurderes når det gjelder forsyningssikkerheten. Risikoanalyser anbefales å gjennomføres som både grovanalyse på et overordnet nivå, og som tematiske risikovurderinger på et detaljert nivå. Virksomheten må uansett gjennomføre en rekke risikovurderinger. Én overordnet fellesvurdering (grovanalyse) er ikke tilstrekkelig for å styre risikoen. Omfanget av risikovurderingene vil variere mellom ulike virksomheter alt ettersom hvor store og komplekse virksomhetene og deres omgivelser er. Små virksomheter kan der det er hensiktsmessig inkludere IKT-sikkerhet i overordnet risikoanalyse.

Alle situasjoner som ikke kan håndteres innenfor ordinær drift i KBO-enhetene, regnes for å være ekstraordinære. En ikke-uttømmende oversikt er listet opp i § 2-6 i kraftberedskapsforskriften. Hvilke situasjoner som regnes som ekstraordinære for KBO-enheten, skal framgå i de årlige risikovurderingene.



**Eksempel: Et nettselskap bestiller risikovurderinger fra et eksternt firma.
Hva må hen passe på i prosessen?**

- Bestiller må ha bestillerkompetanse slik at virksomheten får grundige vurderinger
- Bestiller må ha kompetanse til å forstå innholdet i risikorapporten som leveres
- Vurderingene og videre handlingsplaner må forankres i ledelsen
- Innholdet i rapporten må være lett tilgjengelig og godt kjent av dem som skal bruke kunnskapen
- Nye vurderinger må gjøres minimum årlig
- Kraftsensitiv informasjon må beskyttes i henhold til kap. 6
- Rapporten og oppfølging av rapporten må behandles rett i henhold til internkontrollsystemet (§ 2-10)



Standarder

Risikovurderinger bør bygge på denne standarden framover. Viktigste retningslinje for gode vurderinger.

NS 5814:2021 – Krav til risikovurderinger

NEK EN IEX 31010:2019 Risk management – Risk assessment techniques

NEK EN IEC 60812:2018 Failure models and effects analysis (FMEA an FMECA)

NEK EN 61025:2007 Fault tree analysis (FTA)

NEK EN 61882:2016 Hazard and operability studies (HAZOP studies) – Application guide

NEK EN 62502:2010 Analysis techniques for dependability – Event tree analysis (ETA)

NEK EN IEC 62960:2020 Dependability reviews during the life cycle

Bransjespesifikk veiledning til risikovurderinger

RENB�AD 8064 VEILEDNING TIL RISIKOVURDERING AV 0,23 KV - 24 KV
NETT

Veileder

Vedlegg 1 i NVEs [Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen \(2010\)](#). s. 36-41. Nr.2/2010. **Resten av veilederen er utdatert.**

Krysskobling til annet regelverk

§ 6-9 b i denne forskrift

§ 5-8 i denne forskrift

2.4 Beredskapsplanlegging

§

§ 2-4. Beredskapsplanlegging

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

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

Bestemmelsen skal sikre at virksomheten håndterer ekstraordinære situasjoner effektivt slik at konsekvensene for kraftforsyningen blir minst mulig. Med andre ord er beredskapsplanverket og arbeidet med dette beredskapsleders virkemiddel til å komme raskt i gang med krisehåndtering. Formålet med beredskapsplanverket, er at KBO-enheten skal ha forberedt tiltak som reduserer skade og konsekvenser i ekstraordinære situasjoner. Beredskapsplanverket består som oftest av instruksjer og sjekklister på ulike områder, for eksempel brann i elektrisk anlegg, uvær og IKT-angrep i tillegg til overordnede planer og innsatsplaner. En god beredskapsplan er kortfattet, angir tydelig funksjoner, ansvar og kontaktinformasjon, samt aksjonspunkter dersom en ekstraordinær situasjon oppstår. Beredskapsplanen må inneholde aksjonspunkter for håndtering av restrisiko avdekket etter risikovurderingene iht. § 2-3.

Beredskapsplanverket skal være oppdatert til enhver tid. Dette gjelder også for endring av informasjon i varslingslister. Revisjonsdato skal alltid framgå av planverket.

Beredskapsplanverket skal være lett tilgjengelig og godt kjent av dem som skal bruke planverket. Den kraftsensitive delen av beredskapsplanen skal merkes som nærmere beskrevet i kap. 6-2 i veilederen.

Beredskapsplanverket skal som hovedregel ikke deles med samarbeidspartnere, men like fullt samordnes med berørte myndigheter, andre KBO-enheter og andre relevante samarbeidspartnere. Virksomheten kan velge å dele opp beredskapsplanen i en offentlig versjon som kan deles med samarbeidspartnere, og en del som holdes unntatt offentlighet. Aktuelle samarbeidspartnerne kan for eksempel være: kommuner,

fylkeskommune, hovedredningssentralen, brannvesenet, politi, PST, sivilforsvaret, Forsvaret, Ekom-aktører, NVE, REN, leverandører og KraftCERT for IKT-sikkerhetssituasjoner. De berørte KBO-enhetene er ofte naboenheter eller tilgrensende til hverandres kraftnett. Samordning omfatter å avklare gjensidige forventninger og betingelser for samarbeid og støtte dersom en ekstraordinær situasjon skulle oppstå og beredskapsplanen bli iverksatt. Slik samordning kan for eksempel gjøres i møter med aktuelle aktører.



Eksempel: Innhold i beredskapsplan

- Liste over hvem i virksomheten som kan påkalles ved en situasjon, og hvilken rolle de har
- Liste over myndigheter med kontaktinformasjon som skal varsles ved en situasjon
- Liste over andre KBO-enheter det er aktuelt å varsle avhengig av omfang av situasjonen
- Liste med aktuelle leverandører eller andre som brukes ved feilretting
- Liste over viktige samfunnsfunksjoner som er sluttbrukere
- Kontaktinformasjon / oversikt over sårbare sluttbrukere
- Oversikt over reparasjonsressurser både personell og materiell
- Innsatsplan for tungtransport med nødvendige tillatelser som må iverksettes
- Muligheter for nødaggregat og hvor lenge ulike kommunikasjonsløsninger er i drift ved strømutfall
- Enkel handlingsplan ved driftsstans
- Viktige telefonnumre (brann – politi – ambulanse – lokal kommunal kriseledelse)
- Informasjonsberedskapsplan til egne ansatte og sluttbrukere (ref § 2-8)
- Plan for håndtering av personell ved langvarige beredskapssituasjoner
- Kart over egne anlegg og området virksomheten forvalter



Standarder

NEK EN 60300-3-14:2004 Dependability management – Part 3-14: Application guide – Maintenance and maintenance support
NEK EN 60300-3-16:2008 Dependability management – Part 3-16: Application guide – Guidelines for specification of maintenance support services.
NEK EN 62550:2017 Spare parts provisioning

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

Et varsel er kort informasjon om noe som akkurat har inntruffet før man har full oversikt over situasjonen. Både den første informasjonen som gis til NVE, men også *situasjonsrapporter* underveis, regnes som varsel.

Første varsel

Det første varselet til NVE skal inneholde informasjon om forhold som har eller kan ha betydning for drift og sikkerhet i kraftforsyningen. Alle ekstraordinære situasjoner som gir eller kan gi store samfunnsmessige konsekvenser, konsekvenser for KBO-enheten eller kraftsystemet, skal alltid varsles. En ikke-uttømmende liste over ekstraordinære situasjoner som skal varsles, finnes i § 2-6 bokstav a til h. I tillegg til disse punktene, bør KBO varsle NVE ved situasjoner som beredskapsmyndigheten bør være kjent med, f.eks. om store områder eller viktige samfunnsfunksjoner er berørt. Situasjoner som antas å få medieoppmerksomhet, bør også varsles.

Å varsle uten ugrunnet opphold, vil si å varsle så snart som praktisk mulig. Se egne retningslinjer for varsling og rapportering som sendes til KBO-enheter årlig.

Både NVE og lokalt politi skal varsles ved mistanke om tilsiktet skade eller trussel mot KBO-enhetens anlegg eller systemer.

Varsling kan gjøres på telefon eller via epost. Varsle gjerne ved tvil om varslingsplikt. NVE har utarbeidet en punktliste (se sjekkliste nedenfor) for varsling av situasjoner til NVE.



Sjekkliste: Varsle en situasjon til NVE

Varslet bør inneholde:

- **Hvem** varsler fra hvilken **virksomhet** med hvilken **funksjon** i virksomheten
- Kort om **hva** det gjelder
- **Når** forventer man å ha bedre oversikt over situasjonen
- Hvilke andre **aktører** har eller vil bli varslet i tillegg til NVE



Terskelen for å varsle NVE skal være lav.

Situasjonsrapporter

Situasjonsrapporter er fortløpende varsel under en situasjon. KBO-enheten får beskjed fra NVE om det er behov for oppdatering om utvikling i situasjonen i form av *situasjonsrapporter*. Dette gjelder først og fremst når det er en pågående situasjon, situasjonen er uavklart eller varer over noe tid. NVE kan pålegge KBO-enhetene å sende inn situasjonsrapporter i eget format og til andre tidspunkt enn hva som er vanlig.



Sjekkliste: Pågående situasjon der NVE skal ha situasjonsrapport

Situasjonsrapporten bør inneholde:

- Avsender og andre mottakere enn NVE
- Beredskapsnivå hos avsender
- Hvilket område er berørt
- Eventuelle feil i ledningsnettet eller annet (IKT, trafo m.v.)
- Antall berørte kunder
- Forventet utvikling
- Annen vesentlig informasjon som f.eks.
 - Mannskapssituasjon,
 - Ressurssituasjon
 - Berørte prioriterte kunder
 - Anstrengt kraftsituasjon
 - Behov for rasjonering
 - Behov for samhandling

Hovedregelen er å gi NVE tilstrekkelig informasjon slik at vi kan videreformidle oppdatert informasjon om situasjonen til OED. NVE skal også vurdere behovet for å følge situasjonen framover. Husk at kraftsensitiv informasjon alltid skal behandles i tråd med krav i kapittel 6. Se ellers retningslinjer for varsling og rapportering.

Det er beredskapsvakten i NVE som mottar varsler og situasjonsrapporter fra KBO. Kontaktinformasjon til beredskapsvakten står oppført på NVE sine nettsider.



Er situasjonen varslingsverdig?

I en tidlig fase kan det være vanskelig å vurdere om situasjonen er verdt å varsle NVE. Ved tvil kan det være lurt å informere likevel for å vurdere sammen med NVE om situasjonen skal regnes som ekstraordinær. Om det viser seg at situasjonen ikke utviklet seg til en ekstraordinær situasjon, er det ikke krav til rapportering i etterkant.



Veileder

Retningslinjer for varsling og rapportering.

Retningslinjene er underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2, og unntatt fra innsyn etter offentleglova § 13 og kan ikke deles med andre enn de NVE utpeker som rettmessige brukere av retningslinjene. Retningslinjene vil bli oppdatert årlig, og deles med alle KBO-enheter.

Krysskopling til annet regelverk

Pålegg om å situasjonsrapportere er hjemlet i Enl. § 9.1 4.ledd og § 3-2 i denne forskrift i ekstraordinære situasjoner.

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 andre ledd.

Rapporter etter § 2-6 gjelder situasjoner som er avsluttet, og som NVE skal ha informasjon om. Det er ikke et krav at situasjonen må være varslet på forhånd for at man skal kunne levere en rapport i etterkant. Situasjoner som er listet opp i bokstav a-h, gir en oversikt over hva som minimum må rapporteres. I tillegg kan NVE kreve rapportering av andre tilfeller av uønskede situasjoner enn de som er nevnt i bokstav a-h. KBO-enheten kan også uoppfordret rapportere om forhold som de mener NVE bør kjenne til.

I noen tilfeller vil det være nødvendig for NVE å etterspørre ytterligere informasjon. I slike tilfeller vil NVE ta kontakt med KBO-enheten og be om en nærmere skriftlig redegjørelse. Slike skriftlige redegjørelser vil komme i tillegg til, og ikke i stedet for selve rapporteringen. Sluttrapporten kan være virksomhetens egen evalueringsrapport og/eller utfylt NVE-skjema (Se informasjon om rapporteringsmal i informasjonsboks)

NVE har satt relativt kort frist på rapporteringen for å sørge for at kunnskap om håndteringen av situasjonen ikke går tapt.

Rapportering etter situasjoner brukes blant annet til å se etter mønstre i ulike typer situasjoner på tvers av KBO-enheter. NVE rapporterer slike mønstre tilbake til hele KBO, for eksempel gjennom årsrapporten eller en anonymisert situasjonsrapport. Rapporteringen blir også brukt til å vurdere justeringer i regelverk og tilsyn i tillegg til å løfte problemstillinger som er relevante for kraftforsyningen til andre myndigheter.

Informasjon om hvordan KBO-enhetene sender inn sluttrapporter etter en situasjon er beskrevet nærmere i *Retningslinjer for varsling og rapportering*. Rapporteringsskjema er tilgjengelig på NVE sine nettsider. Om rapporten inneholder kraftsensitiv informasjon, så skal informasjonen beskyttes i henhold til krav gitt i kapittel 6, som er nærmere beskrevet i overnevnte retningslinje for varsling og rapportering. Husk at rapportering skjer til egen e-postadresse. Beredskapsvakta skal ikke ha avsluttede rapporter.



Eksempel: Fysisk innbrudd

Fredag kveld oppdager en ansatt, som jobber ved transformatorstasjonen, at noen har brutt seg inn på anleggsområdet og forsøker å starte en brann på området. Hun skremmer bort brannstifterne med sitt nærvær og varsler raskt beredskapsleder i virksomheten. Ingenting ser ved første øyekast ut til å ha blitt ødelagt. Skal dette varsles og/eller rapporteres til NVE?

Situasjonen har allerede inntruffet. I en tidlig fase er det likevel vanskelig å vite om inntrengerne har rukket å ødelegge noe annet før de ble oppdaget. Dette er en pågående situasjon. Det er viktig å ta rask kontakt med politi slik at de får sikret spor. Varsle også NVE for å vurdere situasjonen. Rapport skal leveres NVE senest innen 3 uker etter situasjonen ble håndtert.

Husk at alle innbrudd, innbruddsforsøk og andre kriminelle forhold alltid skal politianmeldes.

Husk at det finnes en egen e-postkasse i NVE for sluttrapporter. Se NVE sine *retningslinjer for varsling og rapportering*.



Eksempel: IKT-innbrudd

En ansatt oppdager enkelte ødelagte komponenter i transformatorstasjonen mandag morgen. Etter nærmere undersøkelser viser det seg at ødeleggelsene muligens kan kobles til et IKT-innbrudd noen dager tidligere. Vedkommende er i kontakt med IKT-sikkerhetskoordinator i virksomheten som mener forholdet er så alvorlig at han utarbeider en rapport til NVE.

Situasjonen har allerede inntruffet. Det er ikke en pågående situasjon. Husk likevel å varsle KraftCERT så raskt som mulig. Kanskje andre har blitt utsatt for det samme innbruddet. Utstyr har blitt ødelagt. Dette passer i en rapport til NVE. Det er ikke behov for å varsle i tillegg.

Husk at alle innbrudd, innbruddsforsøk og andre kriminelle forhold alltid skal politianmeldes.



Maler

Skjema for rapportering, se to ulike vedlegg på NVE sine nettsider (nederst på nettsiden): <https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/>

Veiledere

Retningslinjer for varsling og rapportering

Retningslinjene er underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2, og unntatt fra innsyn etter offentleglova § 13 og kan ikke deles med andre enn de NVE utpeker som rettmessige brukere av retningslinjene. Retningslinjene vil bli oppdatert årlig, og deles med alle KBO-enheter.

Fjernvarmeberedskap – Veiledning

Se oversikt over hva fjernvarmeselskapene skal rapportere til NVE, s. 12 punkt 7.2.6 i veilederen:

[Fjernvarmeberedskap](#)

2.7 Øvelser



§ 2-7. Øvelser

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

Formålet med bestemmelsen er å sikre at KBO-enhetene vedlikeholder og videreutvikler ferdigheter og prosedyrer som er nødvendige for å håndtere krevende situasjoner. Å definere hensikten med øvelsen og angi klare øvingsmål (læringsmål), som kan evalueres i etterkant, er en svært viktig del av forberedelsene til en øvelse. Identifiser også hvilke indikatorer som kan gi informasjon om målet nås. Flerårsplanen bør inneholde ulike type øvelser slik at man dekker et bredest mulig felt over den gitte tidsperioden.

Øvelsene bør være mest mulig realistiske og ta utgangspunkt i beredskapsplaner (§ 2-4) og informasjonsplaner (§ 2-8). For at læringsutbyttet skal bli bra, bør øvelsene ligne mest mulig på den situasjonen man øver på. Da oppnår man den stressituasjonen en ekte situasjon medfører. KBO-enhetene bør unngå å øve med ressurser som ikke ville vært tilgjengelig i en ekte situasjon. En god øvelse bør inneholde både overraskelser og usikkerhet, og bidra til å teste og forbedre beredskapsplan og innsatsplaner.



Sjekkliste: Formulering av mål etter tankemodellen SMART (DSB)

S	Spesifikt	Tydelig og konkret
M	Målbart	Kvantitative eller kvalitative indikatorer
A	Akseptert	Forankret i organisasjonens ledelse
R	Realistisk	Oppnåelige for utøverne
T	Tidsbundet	Sette en tidsramme for når mål skal være oppnådd

Det er viktig at evalueringsmålene settes allerede i planleggingsfasen av øvelsen.

For at øvelsene skal få et tilstrekkelig innhold og omfang, anbefaler vi å gjennomføre flere øvelser i løpet av året. Hvor omfattende øvelsen(e) må være for å oppnå et godt læringsutbytte, avhenger av den enkelte KBO-enhet og tema. Øvelsene skal dekke relevante tema i fra forskriftens virkeområde. Det er lurt å utarbeide ulike scenarioer som dekker ulike områder som for eksempel natur- eller værutløste situasjoner, teknisk svikt, personellsvikt, IKT-situasjoner og sabotasje. Listen er ikke-uttømmende. Husk å øve på samtidige situasjoner, og/eller sjeldne situasjoner. Både beliggenhet, virkeområde, størrelse på KBO-enheten og funn i risikovurderingene er faktorer som bør ligge til grunn for hvilke øvelser som prioriteres. Husk at hele organisasjonen må øves over tid, inkludert ledelsen. Temaøvelser, som kun berører en liten del av organisasjonen, kan ikke være eneste form for øvelser.

KBO-enheter bør delta på fellesøvelser med aktører man samhandler med. Det skaper arena for bedre koordinering under en reell situasjon. Samhandling regnes som et virkemiddel på veien for å nå et mål.

NVE har utarbeidet veiledningsmateriale for hvordan man kan gjennomføre *øvelser* i kraftforsyningen. Veilederen er listet opp nedenfor. Ved større regionale øvelser bør et eget øvingsdokument beskrive hvilke plikter og rettigheter aktørene har ved alle øvelser i forbindelse med høyspenningsanlegg. Videre anbefaler NVE at det utarbeides en *dreiebok* (prosessverktøy) til bruk i øvelsene.



Veiledere

[Øvelser – En veiledning i hvordan planlegge og gjennomføre øvelser innen energiforsyningen](#). NVE – rapport 39/2015:

[Veileder i planlegging, gjennomføring og evaluering av øvelser – grunnbok \(2016\)](#) – DSB-rapport

[Metodehefte: Spilløvelse \(2016\)](#) – DSB-rapport

2.8 Informasjonsberedskap



§ 2-8. Informasjonsberedskap

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

En informasjonsplan skal bidra til at KBO-enheten deler nødvendig informasjon om pågående situasjoner og håndtering av situasjonene slik at alle involverte parter (både interne og eksterne) har en felles situasjonsforståelse. Informasjonsplanen skal bidra til at beredskapsarbeidet er effektivt og at samarbeidet fungerer godt. Eksempler på eksterne parter er ulike myndigheter, samfunnskritiske virksomheter, andre KBO-enheter, kunder og media.

Informasjonsplanen skal inneholde prosedyrer og planer for hvordan KBO-enheten kommuniserer både internt og eksternt når det er strømløst, når telekom og/eller data helt eller delvis er nede, eller når både strøm, telekom og data er nede.

KBO-enheten bør samarbeide med relevante samarbeidspartnere om informasjonsplanen. Hvilke deler av planen man samarbeider om, vil være avhengig av hvilken aktør KBO-enheten har kontakt med.



Veiledere

[DSB Veileder krisekommunikasjon \(2016\)](#)

2.9 Evaluering

§

§ 2-9. Evaluering

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

Formålet med å evaluere etter øvelser og ekstraordinære situasjoner er å avdekke hvordan virksomheten fungerer i ekstraordinære situasjoner. Dette vil bidra til læring og avdekke behov for endringer på systemnivå samt vurdere grad av måloppnåelse. Alle funn og læringspunkter skal følges opp gjennom en ledelsesforankret tiltaksplan.

Fokuset under evalueringen skal være rettet mot hvordan oppgaver ble håndtert og derav søke å forklare hvilke handlinger som bidro til, eller hindret, måloppnåelse. For best mulig utbytte av øvelser, er det viktig å planlegge evalueringsprosessen samtidig med øvelsesplanleggingen. Før gjennomføring av øvelser, er det viktig å vite hva slags data man trenger for å kunne vurdere måloppnåelse etter øvelsen. Oppfølging av øvelser er først avsluttet når alle punktene i tiltaksplanen er fulgt opp tilfredsstillende.

Gjennom evalueringer kan man avdekke suksesser og feilgrep både på menneskelig, teknisk og organisatorisk nivå. Det er viktig å vite hva man skal bevare og videreføre, og hva som bør endres i håndtering av ulike scenarioer. Det er viktig at forhold som man avdekker i virksomheten, som har forbedringspotensialer, blir trent spesielt på. Dette gjør at man er bedre rustet om en lignende situasjon inntreffer.



Sjekkliste: Hva en evaluering bør inneholde

- Dokumentere hva som har skjedd
- Identifisere hva som fungerte tilfredsstillende – og hvorfor
- Identifisere hva som må endres for å bli bedre
- Oppsummere læringspunkter og forslag til tiltak
- Forankre i ledelsen hvordan læringspunkter og forslag til tiltak skal følges opp videre

Ta gjerne utgangspunkt i S-M-A-R-T (se veiledning til § 2-7 i denne forskrift)

Evalueringen etter en situasjon bør skje raskt etter at normal drift er gjenopprettet. Evaluering etter en øvelse bør skje rett etter at øvelsen er avsluttet. Det er viktig å dokumentere resultatene etter en evaluering. Funn skal følges opp av de som er ansvarlige. Dokumentasjon på hvem som er ansvarlig og hvilke tiltak som skal settes i verk innenfor gitte frister er viktig etter § 2-10.



Veiledere

[DSB Metodehefte: Evaluering av øvelser \(2018\)](#)

2.10 Internkontrollsystem

§

§ 2-10. Internkontrollsystem

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

Internkontrollsystemet skal inneholde dokumentasjon for at alle tiltak etter kravene i første ledd er på plass og fungerer etter sin hensikt. Internkontrollsystemet skal holdes oppdatert og gjennomgås slik at det gjenspeiler faktisk tilstand.

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

Formålet med bestemmelsen er at KBO-enheten skal ha etablert en systematikk som gir en rask og korrekt oversikt over beredskapstilstanden i virksomheten. KBO-enheten skal dokumentere at de følger bestemmelsene i energiloven, energilovforskriften og kraftberedskapsforskriften. Systemet skal kunne gi virksomheten innsikt i om tiltakene som er systematisert fungerer etter hensikten. Det samme systemet skal kunne gi tilsynsmyndigheten en rask og korrekt dokumentasjon over status med hensyn til alle relevante bestemmelser etter denne forskriften.

Systemet må jevnlig oppdateres, gjennomgås og gjenspeile faktisk tilstand.

NVE legger ikke spesielle føringer for hvilken type system KBO-enheten skal bruke eller hvor omfattende dette skal være. Den enkelte virksomhet kan selv bestemme dette. Bestemmelsen gir ingen avgrensning med hensyn til å bruke eller tilpasse allerede etablerte internkontrollsystemer, så lenge bestemmelsens vilkår er oppfylt gjennom å dokumentere at alle krav til beredskap i lov og forskrift er dekket.

Innhold

3. Kraftforsyningens beredskapsorganisasjon (KBO).....	1
3.1 Beredskapsmyndigheten.....	2
3.2 Ansvar og oppgaver for KBO-enhetene.....	4
3.3 Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig	5
3.4 Ansvar og oppgaver for kraftforsyningens distriktssjefer	6
3.5 Fritaksordninger	8
3.6 Sektorvist responsmiljø for IKT-sikkerhetshendelser	12

3. Kraftforsyningens beredskapsorganisasjon (KBO)

Kapittel 3 gir en oversikt over roller og oppgaver som de ulike delene av kraftforsyningens beredskapsorganisasjon (KBO) har. Et velfungerende KBO er et viktig virkemiddel for å sikre en god forsyningssikkerhet av elektrisitet og fjernvarme ved ekstraordinære situasjoner, og sørge for å gjenopprette normaltilstand så raskt som mulig.



Illustrasjon: Logo for kraftforsyningens beredskapsorganisasjon (KBO)

3.1 Beredskapsmyndigheten



§ 3-1. Beredskapsmyndigheten

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

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

Kraftforsyningens beredskapsorganisasjon (KBO) er en nasjonal organisasjon med definert ledelse og struktur. KBO har hjemmel i energiloven § 9-1. Organisasjonen består av både statlige og private aktører. Organiseringen og funksjonsinndelingen i KBO har til hensikt å bidra til å løse kraftforsyningens beredskapsforpliktelser jf. energiloven § 9-2.

Olje- og energidepartementet (OED) har utpekt Norges vassdrags- og energidirektorat (NVE) til å være beredskapsmyndighet med vide fullmakter etter et eget delegeringsvedtak. De områdene der NVE ikke har fått fullmakter etter energiloven, står listet opp i en uttømmende liste i delegeringsvedtaket.

Ved svært store eller krevende situasjoner, kan OED (jf. delegeringsvedtaket) iverksette kraftforsyningens sentrale ledelse (KSL). KSL gis fullmakter ut over hva som reguleres gjennom energiloven og kraftberedskapsforskriften. Mer informasjon om KSLs ansvar og oppgaver følger i § 3-3.

NVE skal administrere KBO og utpeke kraftforsyningens distriktssjefer (KDS) med stedfortredere og inndelege landet i hensiktsmessige KDS-distrikt. NVE kan fastsette forskrift og fatte enkeltvedtak om beredskap i kraftforsyningen. Kraftforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves.

KDS koordinerer KBO-enhetene innenfor sitt geografisk utpekte område (KDS-distrikt). Mer informasjon om KDS sitt ansvar og oppgaver følger i § 3-4.

Bestemmelsen i § 3-1 beskriver beredskapsmyndighetens (NVEs) rett og plikt til å utpeke ledelsen i KBO og samordne beredskapsarbeidet. Den samlede ledelsen i KBO består av kraftforsyningens distriktssjefer (KDS) med stedfortredere, og personer med funksjoner som skal utgjøre kraftforsyningens sentrale ledelse (KSL).

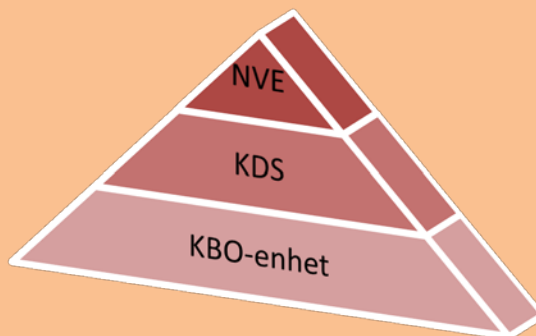
NVE har myndighet til å bestemme at virksomheter skal bli en KBO-enhet, selv om de ikke har klassifiserte anlegg eller system etter kapittel 5 i denne forskrift. Virksomheter som selv mener de har stor samfunnskritisk betydning, kan kontakte NVE for vurdering om de bør bli del av KBO.

Illustrasjon: Organisering av KBO



A

KBO styrt av myndighetene.
Lov og forskrifter tilstrekkelig



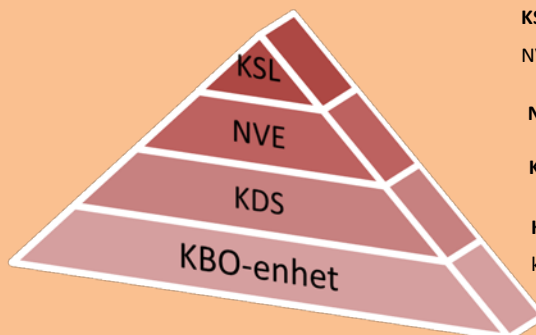
NVE er beredskapsmyndighet

KDS er kraftforsynings
distriktssjefer

KBO-enheter er ulike virksomheter i
kraftsektoren

B

KBO styrt av myndighetene.
Utvidede fullmakter trengs



KSL kan iverksettes av OED og består av
NVE og Statnett ved nasjonale kriser

NVE er beredskapsmyndighet

KDS er kraftforsynings distriktssjefer

KBO-enheter er ulike virksomheter i
kraftsektoren

KBO er normalt styrt av sektorens lover og forskrifter vedtatt av OED (situasjon A). Ved nasjonale kriser kan OED be KSL tre i kraft, for å lede KBO med utvidede fullmakter. Det vil si at virksomhetene i kraftforsyningen blir satt under administrasjon av myndighetene (KSL) (situasjon B). I de aller fleste ekstraordinære situasjoner er sektorlovverket tilstrekkelig for å håndtere situasjonen. NVE utøver sin rolle som beredskapsmyndighet og øverste ansvarlige i KBO, med rapporteringsplikt til OED. Da iverksettes ikke KSL.



Krysskoplinger til annet regelverk

[Delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat \(2019\)](#)

[Energiloven kap.9 Beredskap](#)

3.2 Ansvar og oppgaver for KBO-enhetene



§ 3-2. Ansvar og oppgaver for KBO-enhetene

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

KBO-enheter skal sørge for nødvendig kontakt og samordning med tilgrensende virksomheter og aktuelle KDS.

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

Formålet med denne paragrafen er å understreke at virksomheten er en del av en større organisasjon (KBO), og har oppgaver og plikter i forbindelse med den tilhørigheten.

KBO-enhetene har et selvstendig ansvar for å sørge for god kontakt med nærliggende KBO-enheter eller andre viktige virksomheter i tillegg til KDS. Håndtering under eller gjenoppbygging etter ekstraordinære situasjoner, kan være viktig også for andre tilgrensende KBO-enheter. Den enkelte KBO-enhet skal også kunne forvente at andre KBO-enheter og KDS holder jevnlig kontakt med dem.

Oppgaver som NVE kan pålegge KBO-enhetene å utføre, skal være relatert til ekstraordinære situasjoner eller beredskap enten i forkant, under og/eller etter at hendelsen har inntruffet. Oppgavene skal være nødvendige for å hindre skade eller for å gjenopprette forsyningen så raskt som mulig etter hendelsen.



Krysskopling til annet regelverk

[Energiloven § 9-1 4. ledd](#)

3.3 Ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig



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

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

Departementet kan under beredskap og krig underlegge kraftforsyningen KBO. Kraftforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves. Beredskapsmyndigheten kan instruere KDS og KBO-enheter.

I slike situasjoner overtar KSL ledelsen av KBO. Statnett SF skal i slike situasjoner være KSLs utøvende organ for regulering av produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi.

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

Ved normal drift og i ekstraordinære situasjoner hvor KBO-enhetene, KDS og NVE har tilstrekkelig handlingsrom innenfor energiloven og kbf, er KBO-enhetene kun *del* av KBO.

Ved nasjonale kriser eller krig kan det hende at energiloven og kbf ikke gir tilstrekkelige virkemidler for å håndtere situasjonen. I slike tilfeller kan KBO-enheter og KDS *underlegges* KBO. Det vil si at KSL besluttet iverksatt av OED, og KBO-enhetene i kraftforsyningen underlegges KSL. KSL består av ledere i NVE og i Statnett SF. KSL sørger da for å iverksette nødvendige tiltak i henhold til denne forskrift § 3-3 første ledd. KSL vil holde departementet underrettet om kraftforsyningssituasjonen på samme måte som NVE vanligvis gjør det i ekstraordinære situasjoner innenfor lov og forskrift.

Energiloven §§ 9-1 og 9-4 gir til sammen NVE mulighet til å overføre sin vedtaksmyndighet til KBO under beredskap og krig jf. kbf § 3-3. Formålet med en slik delegeringsmulighet er å kunne ivareta forsyningssikkerheten i den rammede regionen dersom sentrale myndigheter (NVE/KSL) ikke lenger er i stand til dette. KDS har de beste forutsetningene til å kunne påta seg en slik myndighet, siden de i dag allerede har en koordineringsfunksjon i sitt distrikt. Dette er nærmere angitt i § 3-4 i siste del av andre ledd. Forskrift om planlegging og gjennomføring av rekvisisjon av kraft og tvangsmessige leveringsinnnskrenkninger ved kraftrasjonering (kraftrasjoneringsforskriften) gjelder også.

KBO-enheter plikter å rette seg etter pålegg og vedtak fra KSL eller KDS og etterkomme kravene innen frister som er gitt. Det er viktig å presisere at ingen KBO-enhet i slike situasjoner skal avvende eventuelle pålegg og vedtak fra KSL eller KDS, men gjøre det som er nødvendig for å opprettholde normal drift så lenge som mulig.

I § 3-3 fjerde ledd vises det til at Statnett SF har regionale representanter med myndighet når KSL er satt. Det vil si at KBO-enheter må være godt kjent med hvilke(t) KDS-distrikt de tilhører, og hvilke(n)

regional representant i Statnett SF man skal forholde seg til. KDS må også ha tilstrekkelig kjennskap til Statnett SF sine regionale representanter.



Krysskoplinger til annet regelverk

[Energiloven § 9-1 siste ledd](#)

[Energiloven § 9-4](#)

[Delegering av myndighet etter energiloven til Norges vassdrags- og energidirektorat \(2019\)](#)

[Forskrift om kraftrasjonering \(Kraftrasjoneringsforskriften\)](#)

Lovverk av betydning også for kraftforsyningen ved krig eller fare for krig

[Lov om særlige rådgjerd under krig, krigsfare og liknende forhold \[beredskapsloven\]](#)

[Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret \(sivilbeskyttelsesloven\)](#)

3.4 Ansvar og oppgaver for kraftforsyningens distriktssjefer



§ 3-4. Ansvar og oppgaver for KDS

Beredskapsmyndigheten skal beslutte inndeling av distrikter og utpeker KDS med stedfortredere.

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

Formålet er å definere KDS sitt ansvarsområde og understreke hvilke oppgaver som hører til KDS-funksjonen. Første ledd viser til at det er NVE som har ansvar for å inndeles KDS-distriktene i hensiktsmessige områder og som bestemmer hvilke personer som skal ha funksjonen som KDS og stedfortredende KDS. NVE kan be om innspill til både distriktsinndeling og hvem som bør tildeles dette

ansvaret. KDS kan ikke endre områdegrensene eller velge hvem som skal inneha rollene uten godkjenning fra NVE.

KDS utpekes som hovedregel fra en KBO-enhet som driver det regionale nettet innenfor et større område (distrikt). Normalt legges KDS-funksjonen til den virksomheten som ivaretar myndighetspålagte energiutredninger i området (jf. forskrift om energiutredninger). NVE kan fravike denne hovedregelen.

Inngåtte avtaler mellom KDS, stedfortreder og NVE regulerer KDS-funksjonen sine oppgaver i normalsituasjon og i ekstraordinære situasjoner både regionalt og nasjonalt. KDS-avtalen er gjensidig oppsigelig.

Årlige forventningsbrev fra NVE beskriver også oppgaver NVE forventer at KDS setter på dagsorden det året. KDS har plikt til å oppfylle inngåtte avtaler og oppgaver i forventningsbrevet.

KDS-oppgaver:

KDS er NVEs representanter på regionalt nivå i ekstraordinære situasjoner. Kort fortalt skal KDS ha et koordinerende ansvar for å sikre godt samarbeid mellom ulike aktører i sin region. KDS representerer NVE i alle fylkesberedskapsråd angående spørsmål som har med kraftforsyningen å gjøre. KDS-ene skal ha oversikt over de viktigste beredskapsmessige utfordringene innenfor sine distrikter, tilrettelegge for samhandling mellom KBO-enhetene og bidra med råd og veiledning om sikringstiltak og beredskap der det er naturlig.

NVE har myndighet til å delegere ytterligere oppgaver til KDS uavhengig om det er en ekstraordinær situasjon. NVE kan delegere fullmakt til å fatte vedtak i sitt distrikt, til KDS (jf. enl. § 9-4). KDS har i slike situasjoner myndighet til å fatte vedtak overfor alle KBO-enheter innenfor sitt distrikt på vegne av NVE. Sitat energiloven § 9-4, 2. ledd:

«Forvaltningsloven kapittel II om ugildhet gjelder ikke for saker som behandles av KBO. Saker skal uansett forberedes og avgjøres etter en forsvarlig, saklig og nøytral saksbehandling»

Les mer om delegering av myndighet under veiledning til § 3-3.

NVE forventer at KBO-enhetene i et distrikt møter når KDS innkaller til samarbeidsmøter. Alle KBO-enheter plikter å svare på henvendelser fra KDS i forbindelse med ekstraordinære hendelser der KDS er satt til å koordinere situasjonsrapporteringen. Se retningslinjer for varsling og rapportering. KDS plikter på sin side å ha kapasitet til å ivareta en koordinerende rolle. NVE kan alternativt be om situasjonsrapportering direkte fra KBO-enhetene inn til NVE. I så fall sendes situasjonsrapporteringen fra KBO-enhetene til KDS for kommentar.



KDS-rollen må rapportere inn oppdatert kontaktinformasjon. Dette gjøres ved å fylle ut Skjema for innrapportering av kommunikasjonsmidler KDS.

<https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/>

Kostnader til KDS-arbeidet dekkes gjennom inntektsrammereguleringen. Alt som legges til grunn for beregning av inntektsrammen rapporteres igjennom eRapp.



Krysskoplinger til annet regelverk

[Forskrift om energiutredninger](#)

[Forskrift om økonomisk og teknisk rapportering, inntektsramme for nettvirksomheten og tariffer](#)

[Pålogging til eRapp – NVE](#)

<https://www.nve.no/reguleringsmyndigheten/regulering/nettvirksomhet/oekonomisk-regulering-av-nettselskap/rapportering-av-data/oekonomisk-og-teknisk-rapportering/paalogging-til-erapp/>

Veileder

[Retningslinjer for varsling og rapportering](#)

Retningslinjene er underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2, og unntatt fra innsyn etter offentleglova § 13 og kan ikke deles med andre enn de NVE utpeker som rettmessige brukere av retningslinjene. Retningslinjene vil bli oppdatert årlig og delt med alle KBO-enheter.

3.5 Fritaksordninger

§

§ 3-5. Fritaksordninger

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

Forsvarsloven gir hjemmel til å disponere nødvendig personell for å sørge for Forsvarets operative evne

og sikre egnet bemanning. For å sørge for tilstrekkelig bemanning i kraftforsyningen ved mobilisering og krig, er det utarbeidet en egen unntaksbestemmelse for KBO.

Kraftberedskapsforskriften § 3-5 synliggjør muligheten til å søke om fritak. Søknad utarbeides og sendes av den enkelte KBO-enheten til forvalter av aktuell fritaksordning. Alle KBO-enheten er registrert som samfunnsskrittiske virksomheter hos Forsvaret.

Nedenfor gir vi en kort oversikt over fritaksordningene. Ellers viser vi til veiledningsmateriale utarbeidet av Forsvaret.

Utsettelse eller fritak for fremmøte i Forsvaret

Søknad om fritak behandles etter reglene i vernepliktsforskriften kapittel 11. Forsvaret, gjennom Forsvarets personell- og vernepliktsenter, kan etter søknad innvilge mobiliseringsfritak (eller -utsettelse), for personell som er nødvendig for driften av kraftforsyningen.

Forutsetningene for at det gis fritak for frammmøte i Forsvaret etter vernepliktforskriften er at

- arbeidstakeren har fullført førstegangstjenesten
- arbeidstakeren har fått et disponeringskort eller en innkalling til Forsvaret
- arbeidstakeren dekker en kritisk funksjon i virksomheten
- virksomheten dekker en samfunnsskrittisk funksjon, og er registrert som samfunnsskrittiske virksomheter (SKV)
- arbeidstakeren er disponert eller planlagt disponert i Forsvarets styrker, Heimevernet inkludert, har fått brev om nytilføring til Heimevernet eller er innkalt til repetisjons-/hjelpetjeneste

For å oppfylle tredje kulepunkt bør KBO-enheten ha utarbeidet et beredskapsplanverk hvor vedkommende sin funksjon i beredskapsorganisasjonen framgår, og en plan for hvordan personellbehovet ved krigsberedskap skal dekkes. Hjemmelen om å søke fritak gjelder for alle enhetene i KBO.

Begreper og roller iht. vernepliktsforskriften	Aktør i kraftbransjen	Oppgaver
Samfunnsskrittisk virksomhet «SKV»	KBO-enhet	- Sendersøknad til vernepliktsverket om fritak for eget personell. - Informerer Forsvaret om avgang/fratredelse av personell - Ta kontakt med NVE for avklaring ved behov for fritak av kritisk personell fra leverandør.
Koordinerende forvaltningsorgan «KFO»	NVE	- Informerer Forsvaret om endringer i KBO (og dermed hvilke virksomheter som ansees som «SKV»)
Departementene	OED	- Informerer Forsvaret om at NVE er «KFO»

For nærmere informasjon se Forsvaret sine nettsider: www.forsvaret.no/fritaksordningen

Fritak for tjeneste i Sivilforsvaret og Politireserven

Etter *forskrift om sivilforsvar* kan nøkkelpersonell i kraftforsyningen fritas for tjeneste i Sivilforsvaret. Ordningen er ment å gi fritak for det personellet som er viktigst og vanskeligst å erstatte innen drift, feilretting, vedlikehold og økonomi og administrasjon.

Den enkelte KBO-enheten skal ved innkalling sende skriftlig melding til aktuell sivilforsvarskrets om hvilket nøkkelpersonell som ønskes fritatt for tjeneste i Sivilforsvaret. Meldingen skal inneholde nødvendige opplysninger. Dette er navn, fødselsnummer (11 siffer) og stilling i virksomhetens beredskapsorganisasjon. Ved fratredelse i fritaksberettiget stilling, plikter både den enkelte og virksomheten å underrette sivilforsvarskretsen om det.

Politireserven ble avviklet på oppdrag fra Justis og beredskapsdepartementet i 2020.¹



En KBO-enhet kan bare søke fritak fra tjeneste i Forsvar eller Sivilforsvaret for egne ansatte. Fritaksordningen gjelder som hovedregel ikke innleid personell. Ved behov for fritak av kritisk viktig personell hos leverandør, så ta kontakt med NVE for nærmere avklaring.



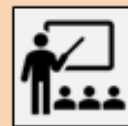
Eksempel: Arbeidstakeren dekker en kritisk funksjon i virksomheten

Virksomheten har to faste montører som kan reparere ødelagte kraftledninger ved utfall eller andre feil. En av montørene ansatt i KBO-enheten, som har gjennomført førstegangstjenesten, får mobiliseringsvarsel fra Forsvarets personell og vernepliktssenter. KBO-enheten har avtaler med to andre virksomheter om felles disponering av montører som kan reparere ødelagte punkter i kraftnettet. Dekker arbeidstakeren en kritisk funksjon i virksomheten?

Etter NVEs mening:

Ja. Vedkommende har spesialkompetanse som ikke lett kan erstattes av andre. Vedkommende er også definert av OED som samfunnskritisk personell og er beskrevet nærmere i virksomhetens beredskapsplanverk. For å sikre tilstrekkelig kjennskap til nettet i virksomheten har ikke virksomheten noe å gå på om en blir syk. NVE vil i slike tilfeller anmode Forsvaret eller sivilforsvaret om å regne vedkommende som å inneha en samfunnskritisk funksjon.

¹ www.politiet.no/globalassets/05-om-oss/rapporter/politiets-arsrapport-2020.pdf



Eksempel: Arbeidstakeren dekker ikke en kritisk funksjon i virksomheten

KBO-enheten har en sentralbordoperatør. Sentralbordfunksjonen er viktig for virksomheten både til vanlig og under ekstraordinære situasjoner. Vedkommende har gjennomført førstegangstjeneste og får mobiliseringsvarsel fra Forsvarets personell og vernepliktsenter. Sentralbordfunksjonen er ikke beskrevet som en viktig funksjon i virksomhetens beredskapsplanverk. Dekker arbeidstakeren en kritisk funksjon i virksomheten?

Etter NVEs mening:

Nei. Det krever ikke lang spesialkompetanse å operere et sentralbord. Så lenge virksomheten heller ikke har definert rollen som samfunnskritisk i sitt beredskapsplanverk, regnes ikke vedkommende for å inneha en samfunnskritisk funksjon. Det forventes at virksomheten er i stand til å lære opp personer i bruk av sentralbordet innenfor relativt kort tid. Det forventes også at det er personer som allerede kan funksjonen og som brukes ved behov. NVE vil i slike tilfeller ikke anmode Forvaret eller sivilforsvaret om å regne vedkommende som å inneha en samfunnskritisk funksjon.



Informasjonsskriv fra OED om hvem som regnes som driftskritisk personell i KBO-enhetene:

[Ansatte i kritiske samfunnsfunksjoner](#)

Krysskoplinger til annet regelverk

[Lov om verneplikt og tjeneste i Forsvaret m.m. \(forsvarsloven\)](#)

www.forsvaret.no/fritaksordningen

[Generelt om fritaksordningen ifølge vernepliktsforskriften](#)

[Virksomhetens plikter ifølge vernepliktforskriften](#)

[Forskrift om sivilforsvar \(sivilforsvarsforskriften\) - Lovdata](#) Se spesielt kap 4 Midlertidig fritak fra tjeneste i Sivilforsvaret [Veileder til forskrift om sivilforsvar | Direktoratet for samfunnssikkerhet og beredskap \(dsb.no\)](#)

www.sivilforsvaret.no/innkalt-for-forste-gang/fritak-fra-tjeneste-i-sivilforsvaret/

Se ellers § 2.4 Beredskapsplanlegging

3.6 Sektorvist responsmiljø for IKT-sikkerhetshendelser



§ 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.

NVE er som beredskapsmyndighet, utpekt til sektorvist responsmiljø (SRM) for IKT-sikkerhetshendelser i kraftforsyningen. Funksjonen bør forstås i forlengelsen av NVEs øvrige beredskapsoppgaver med hensyn til forsyningssikkerhet. Ordningen skal i utgangspunktet omfatte samtlige virksomheter som er underlagt denne forskriften.

Krav til grunnleggende kapasitet for et sektorvist responsmiljø er beskrevet i NSM sitt rammeverk for håndtering av IKT-hendelser. Oppgavene er gitt i form av en prosessbasert modell hvor følgende trinn inngår:

- 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
- 6) Tilbakeføring og læring av hendelsen

NVE har delegert deler av oppgavene til KraftCERT. Den pålagte hovedoppgaven til KraftCERT er å samle, systematisere, analysere, vurdere og dele IKT-sikkerhetsinformasjon om sårbarheter, trusler og hendelser som kan ramme informasjons- og styringssystemer. Som SRM, ivaretar NVE kommunikasjon til departementet (OED) og sikkerhetsmyndighetene (NSM og PST), mens KraftCERT har en teknisk-operativ funksjon, og samarbeider med andre CERTer nasjonalt og internasjonalt. Både NVE og KraftCERT er partner i det nasjonale cybersikkerhetssenteret (NCSC).

**Veiledere**

[NSM: Rammeverk for håndtering av IKT-sikkerhetshendelser](#)

Nettsted

[KraftCERT](#)

Innhold

4. Ressurser og reparasjonsberedskap	1
4.1 Reparasjonsberedskap	1
4.2 Kompetanse og personell	3
4.3 Drift i ekstraordinære situasjoner og gjenoppretting av funksjon	6
4.4 Materiell og utstyr	9
4.5 Transport	14
4.6 Nasjonal tungtransportberedskap	19
4.7 Samband	20

4. Ressurser og reparasjonsberedskap

Kapitlet beskriver beredskapen som KBO-enheter må ha for å kunne redusere konsekvensene dersom en ekstraordinær hendelse inntreffer. Kapitlet stiller krav til KBO-enhetenes organisering, kompetanse og ressurser. Forklaring av begrepet *ekstraordinære situasjoner* finner du i ordforklaringer til § 1-1. *Formål.*

Kapitlet beskriver videre hvilke nødvendige komponenter og utstyr til gjenoppretting KBO-enhetene må ha tilgang til. Dette inkluderer anleggsdeler, verktøy, transportutstyr, sambandsutstyr og annet relevant utstyr.

4.1 Reparasjonsberedskap



§ 4-1.Reparasjonsberedskap

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

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

Hensikten med reparasjonsberedskap er først og fremst å redusere konsekvenser av feil og skader på anlegg og komponenter. Reparasjonsberedskapen skal stå i forhold til alle former for ytre påkjenninger og i forhold til risiko for ekstraordinære hendelser. Reparasjonsberedskapen må dimensjoneres etter hva slags anlegg virksomhetene har, som for eksempel sjøkabler og fjordspenn, anleggets klasse og samfunnsskrittiske betydning.

Organiseringen skal være slik at drift og reparasjon er så effektiv som mulig i og etter ekstraordinære situasjoner. KBO-enheter trenger ikke å ha alle ressurser selv. Tilgang til personell, materiell og utstyr kan avtales med andre.

Bestemmelsen innebærer også krav til utholdenhet. For å være utholdende, må enheten ha planer, ressurser og personell for å håndtere langvarige og omfattende hendelser, og med flere samtidige hendelser. Planene skal beskrive hvordan drift og gjenoppretting kan skje og hva som er nødvendige ressurser under ekstraordinære situasjoner.



Eksempler på samtidige hendelser

Uvær ødelegger kraftledninger og ekom

En storm fra nordøst, som ikke er vanlig vindretning, ødelegger både luftledningsmaster og basestasjoner for KBO-enhetens eget samband. Uværet er uvanlig kraftig der KBO-enheten er lokalisert. Den har mannskap som kan reparere kraftledninger, og underveis i reparasjonsarbeidet er det viktig å ha god kontakt mellom driftssentralen og mannskapet. Uten ekom-forbindelse er det ikke mulig å opprettholde kontakten hverken med driftsradio eller mobiltelefon. Dekningen for nødnettet er dårlig. KBO-enheten må planlegge hvordan arbeid i felt kan skje sikkert, selv om mannskapet er avskåret fra normal kommunikasjon.

Rasjonering med uvanlig mange koblinger i nettet og feil på mange komponenter

Ved rasjonering blir det mange flere koblinger og belastningsendringer. Flere koblinger gir flere feil på brytermateriellet. Dette er et sammenfall mellom to hendelser, der den ene fører til den andre – rasjonering og mange koblinger. Dette betyr at det må være økt reparasjonsberedskap for brytermateriellet under rasjonering med sonevis roterende utkobling.

Transformatorhavari og ødelagt vei

En av hovedtransformatorene får vindingskortslutning og den må fraktes til transformatorverksted for å få ny vikling. Kort etter går en lokal elv over sine bredder og vasker vekk deler av veien inn til stasjonen slik at det vil ta lang tid før veien er kjørbær for transformatortransport. Virksomheten må da greie seg uten erstatning i lenger tid enn planlagt. Dette betyr at denne hendelsen burde vært risikovurdert, konsekvensene vurdert og beredskap planlagt. Er det mulig å reparere på stedet? Er det redundans i nettet? Vil hendelsen ramme samfunnsskrittiske funksjoner? Er det mulig å få veien reparert raskt?

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

Enhetene må analysere hvilke hendelser som skal være dimensjonerende for reparasjonsberedskapen. *Alle ekstraordinære situasjoner* betyr at det må planlegges for omfattende ødeleggelser. Energiforsyningen skal gjenopprettes uansett hva som er årsaken til avbruddet. Omfattende ødeleggelser vil ta lenger tid og kan kreve store ressurser.

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



Krysskopling til annet regelverk

[Forskrift om kraftrasjonerings \(kraftrasjoneringsforskriften\)](#)

4.2 Kompetanse og personell



§ 4-2. Kompetanse og personell

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

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

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

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

KBO-enheter skal ha egne ansatte som utgjør kjernen i det som kreves for å håndtere ekstraordinære situasjoner. Ytterligere tilgang på personell med kompetanse kan sikres både gjennom pålagt overtid for eget personell, avtale om innleid personell eller gjennom samarbeidsavtaler. Når KBO-enheter velger å bruke innleid personell, må det inngås en bindende avtale om sikker tilgang til dette personellet. Legg merke til at kompetansekravet blant annet omfatter forhold som:

- Kriseledelse
- Sikring og drift av anlegg i ekstraordinære situasjoner, herunder produksjon, nett, fjernvarme, driftskontrollsystemer og samband
- Gjenoppretting og reparasjon
- Krisekommunikasjon (se også §2-8. *Informasjonsberedskap* og § 7-17. *Mobile radionett – driftsradio*)



Eksempel

I ett av koblingsanleggene har Strøm Nett to gamle trykkluftbrytere. Selv om de har to trykkluftbrytere, er det ingen i virksomheten som kan reparere dem hvis de svikter. Ved brytersvikt blir flere avganger til lokal forsyning uten spenning. Strøm Nett har derfor inngått en beredskapsavtale med et firma som kjenner teknologien. Avtalen sikrer oppmøte av kompetent personell innen 8 timer. I avtalen inngår også årlig kontroll og vedlikehold. Strøm Nett vurderer å bytte bryterne til en type som de selv har kompetanse på, og som er enklere å reparere og vedlikeholde.

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

Leder for virksomheten, beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator må ha nødvendig kompetanse og utgjør kjernen for styring av enheten gjennom ekstraordinære situasjoner. Energilovforskriften § 3-6 om tilgang til personell krever at nettselskaper med inntektsramme har tilstrekkelig egenbemanning til å lede virksomheten i enhver situasjon. Energilovforskriften krever ikke det samme av kraftprodusenter og fjernvarmevirksomheter, men kraftberedskapsforskriften har krav til at alle KBO-enheter har etablert en organisasjon og har personell med kompetanse for å håndtere ekstraordinære situasjoner.

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

Det skal foreligge planer for å dekke personellbehovet til de ulike funksjonene i ekstraordinære situasjoner.

- Oversikt over tilgjengelig personell til å dekke nødvendige funksjoner i en ekstraordinær situasjon
- Personellet's funksjon og eventuell spesialkompetanse
- Nødvendig kontaktinformasjon

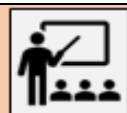


Eksempel

Strøm Nett og flere andre KBO-enheter i distriktet har inngått en avtale om å bistå hverandre ved større hendelser; deriblant to produksjonsselskaper og flere nettselskaper. På denne måten øker sikkerheten for at ikke alle rammes på likt av samme hendelse. Noen av KBO-enhetene har god bemanning, mens andre leier inn entreprenører. De har passet på at ikke alle har beredskapsavtale med den samme entreprenøren.

Beredskapslederne og beredskapskoordinatorene møtes etter store hendelser for å evaluere om ordningen fungerer tilfredsstillende.

I den utstrekning KBO-enheter er avhengig av personell utenfor egen virksomhet, må de utarbeide personellplaner for disse. KBO-enhetene må inngå avtaler som sikrer dem prioritet til det innleide personellet i ekstraordinære situasjoner. Det må skaffes sikker tilgang til personell som ikke er en del av egen grunnbemanning ved avtaler. Slike avtaler kan inngås med andre KBO-enheter, eller driftsselskaper, entreprenørselskaper og leverandører.



Eksempel

Strøm Fjernvarme er helt avhengig av den største oljekjelen hvis de skulle få feil på en av de andre kjelene. Beredskapskoordinatoren har vurdert avtalen de har med firmaet som har levert kjelen, og ser at hvis de får feil, så kan de kontakte firmaet i arbeidstiden. Firmaet garanterer da å ha en reparatør på plass innen to døgn. Beredskapskoordinator og beredskapsleder i Strøm Fjernvarme innser at med en slik ordning, får de store problemer hvis en feil skjer rett før en helg eller høytid. Skjer feilen fredag nær arbeidstidens slutt, får de ikke kontakt før mandag morgen, og reparasjonen kan tidligst begynne onsdag. Strøm Fjernvarme bestemmer seg derfor for å kjøpe utvidet beredskap med kontaktmulighet alle dager, og at reparasjon skal påbegynnes senest innen ett døgn.

4.3 Drift i ekstraordinære situasjoner og gjenoppretting av funksjon



§ 4.3 Drift i ekstraordinære situasjoner og gjenoppretting av funksjon

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

I denne bestemmelsen konkretiseres at KBO-enheter skal drive anleggene og gjenopprette funksjoner. Til dette skal den organisasjonen som er omtalt i § 4-1 brukes; personell som har riktig kompetanse etter § 4-2 være tilgjengelig; og materiell og utstyr som angitt i § 4-4 stå til rådighet.

For å oppfylle kravet, må KBO-enheter

- ta hensyn til at spesielle forhold som ekstremvær kan forsinke gjenopprettingen, men at gjenopprettingen likevel skal skje så snart som mulig
- ta hensyn til påregnelige praktiske eller tekniske vansker ved gjenoppretting
- sikre at det er så mange personer tilgjengelig at det blir mulig å opprettholde arbeidet gjennom langvarige situasjoner
- kunne håndtere ekstraordinært press over lang tid
- ta høyde for at det kan oppstå flere samtidige hendelser
- sørge for at personell ikke skades

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

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

Reparasjonsberedskap i transmisjonsnett og regionalt distribusjonsnett med tilgrensende kraftstasjoner

Nødvendige ressurser må være tilstrekkelige og tilgjengelige i ekstraordinære situasjoner. KBO-enheter bør på forhånd gjennomføre en egen vurdering og bestemme akseptabel responstid for startfasen etter en uønsket hendelse, og dokumentere dette i beredskapsplanen.

Når det er redundans i kraftsystemet, skal forsyningen gjenopprettes øyeblikkelig og automatisk, eller ved kobling. Ved radiell forsyning skal KBO-enheter legge stor vekt på å ha forberedt provisorisk

forsyning. I enkelte feiltilfeller hvor det i utgangspunktet er bygget med redundans, kan likevel funksjonen rammes hvis flere redundante komponenter rammes.

Den følgende skissen til responstider er hentet fra rapporten [Reparasjonsberedskap i sentral- og regionalnettet og tilknyttede kraftstasjoner](#), Oslo desember 2011. Rapporten er utarbeidet gjennom et samarbeidsprosjekt mellom NVE, Statnett, nettvirksomheter og produksjonsvirksomheter oppnevnt av Energi Norge, Samfunnsbedriftene og Distriktsenergi.

Skisse til responstider



Feilretting når driftskontrollsystemet er i klasse 3

- oppdage hendelsen straks i driftssentral og driftskontrollsystem, jf. § 5-6, vedlegg 3 Særlige krav til sikring for anlegg klassifisert i klasse 3
- vurdere situasjonen og foreta omkobling så raskt som fysisk mulig for å gjenopprette forsyningen anslagsvis 1 minutt til 1 time
- i stasjonsanlegg kan det være nødvendig å sende ut mannskap så raskt som fysisk mulig for å se omfanget og hvilken del av stasjonsanlegget som er ”friskt” før innkobling foretas, ½ - 1 time
- videre reaksjonsmønster i henhold til beredskapsplan, se § 2-4
- kun unntaksvis skal sluttbrukere være uten strøm i mer enn 1-2 timer ved feil i transmisjons- og regionalt distribusjonsnett. Hvis dette ikke er tilfelle, se feil som medfører avbrudd i forsyningen nedenfor

Etter gjennomført startfase kan det ta dager til måneder for å gjenopprette status som før feilen oppstod. Se nedenfor om reparasjonsfasen

Feilretting når driftskontrollsystemet er i klasse 2

- oppdage hendelsen raskt i driftssentral og driftskontrollsystem, anslagsvis 1 til 15 minutter, se § 5-5. *Sikringstiltak for klasse 2*
- vurdere hendelsen og iverksette innledende tiltak uten ugrunnet opphold, anslagsvis 10 til 15 minutter
- videre reaksjonsmønster i henhold til beredskapsplan, se § 2-4

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

Feilretting når driftskontrollsystemet er i klasse 2 og 3 - Feil som medfører avbrudd i forsyningen til kunder

- oppdage og vurdere hendelsen – se over
- bestemme innledende tiltak, anslagsvis 5 til 15 minutter
- innkalle mannskap for kriseledelse, lokalisering av feil med mer, anslagsvis 15 minutter
- mannskap klar for utrykking, anslagsvis 15 minutter til 2 timer
- kartlegge og vurdere hendelsen i detalj, fra timer til døgn, avhengig av tilgjengelighet, værforhold, risiko ved befarings og andre forhold på stedet
- reparasjon av ødelagt anlegg eller komponent, fra timer til måneder
- provisorisk løsning etableres for å gjenopprette forsyningen, anslagsvis 4 timer til 1 døgn

- gjenopprette forsyningen provisorisk fra en helt ødelagt transformatorstasjon, 3 til 4 døgn

Avbrudd med stort omfang

- innledende faser som over
- etablere krisestab
- sende ut mannskap for å se omfanget og vurdere tiltak, anslagsvis ½ til 2 timer avhengig av vær
- innkalle beredskapsressurser (materiell og mannskap)
- iverksette eventuelle midlertidige løsninger (kabler på bakken, forbikobling, provisoriske koblingsanlegg)

Reparasjonsfasen

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

Produksjonsanlegg i klasse 2 og 3

- oppdage hendelsen raskt/straks i driftskontrollsystemet
- vurdere situasjonen, iverksette innledende tiltak uten ugrunnet opphold/så raskt som fysisk mulig
- foreta omkobling for å gjenopprette mest mulig av forsyningen, 1 minutt til 1 time
- det kan være nødvendig å sende inn mannskaper for å se på omfanget og hvilke deler av anlegget som er "friskt" for innkobling, ½ til 3 timer
- gjøre beslutninger om videre tiltak, neste arbeidsdag
- innkalle relevante beredskapsressurser (materiell og mannskap)
- igangsette reparasjonsarbeider

Deretter kan det ta fra dager til måneder for å gjenopprette status som før feilen oppstod.

Reparasjonsberedskap for lokalt distribusjonsnett og fjernvarme

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

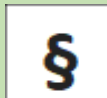
- oppdage feil raskt
- gjøre innledende vurderinger
- lokalisere feil-sted
- sende ut mannskap for å starte med reparasjoner uten ugrunnet opphold
- iverksette midlertidige løsninger hvis avbrudd kan forventes å vare i mer enn noen timer

Det bør tilstrebes samme responstider som for transmisjons - og regionalt distribusjonsnett. I tillegg bør det i lokalt distribusjonsnett legges vekt på aggregatdrift inntil feil er reparert, for at samfunnsviktige funksjoner kan opprettholdes.



NVE presiserer at alle kunder som er kritisk avhengige av kontinuerlig strømforsyning, selv har ansvar for å sikre egen nødstrøm.

4.4 Materiell og utstyr



§ 4-4 Materiell og utstyr

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

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

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

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

Komponenter som det er vanskelig å skaffe eller som har lang leveringstid, må være tilgjengelig i et beredskapslager.

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

Et viktig forhold er at det skal være sikker tilgang til materiell og utstyr i en ekstraordinær situasjon uavhengig av om ressursene eies av KBO-enheten eller av andre.

Reservemateriell

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

- beredskapsmaster
- reservetransformatorer, transformatorolje og liknende
- kabellengder og skjøter (sjø, luft, fjordspenn og liknende)
- komponenter som effektbrytere, kompressorer, isolatorer og liknende
- fjernvarmerør, ventiler og pumper
- mobile varmesentraler
- datakomponenter og programvare for kritiske funksjoner

Utstyr

Enheten må ha tilgang til alt nødvendig utstyr som trengs for å opprettholde kraftforsyningen i ekstraordinære situasjoner, og for å gjenopprette funksjon. Dette kan være verktøy, maskiner eller annet som er nødvendig for å foreta reparasjoner, gjenoppretting eller iverksette midlertidige tiltak. Eksempler på nødvendig utstyr kan være:

- transportutstyr og maskiner
- kraner og annet utstyr som er nødvendig for tunge løft
- aggregater
- verktøy for reparasjonsarbeid
- sikkerhetsutstyr

Reservemateriell og utstyr kan sikres gjennom avtale med andre

Kravene til reservemateriell og utstyr kan etterleves enten gjennom at KBO-enheten selv har tilstrekkelig med utstyr og materiell eller gjennom skriftlige avtaler med leverandør, samarbeidsordninger, som eksempelvis REN Beredskap, eller andre. Det vil være avgjørende med tilstrekkelig klare avtaler og at eventuelle samarbeidsordninger har et omfang og et innhold som gjør tilgangen på utstyr og reservemateriell sikker etter de risikovurderinger som er gjort.



Enheten må sørge for at leverandører av kritisk viktige komponenter forplikter seg til å

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

Forsvarlig stand

Materiell og utstyr som er nødvendig for sikrings- og beredskapstiltak, skal holdes i forsvarlig stand slik at det fungerer etter forutsetningen i ekstraordinære situasjoner. KBO-enheter må derfor gjennomføre systematisk vedlikehold og modernisering eller erstatte gammelt utstyr med nytt, slik at utstyret fungerer etter hensikten når behovet oppstår. KBO-enheter bør legge spesiell vekt på dette for utstyr som sjelden er i bruk. Materiell og utstyr må lagres på en forsvarlig måte etter de anvisninger som er gitt fra fabrikanten. Ofte vil det være på sin plass å ha et eget lager for materiell og utstyr som skal brukes i ekstraordinære situasjoner. Se også § 5-1 Sikringsplikt.



Utstyr som sjelden brukes

Hvis utstyret er sjelden i bruk, kan kunnskapene om hvordan det brukes, gå tapt. Dessuten finnes det utstyr som har komponenter med begrenset holdbarhet slik at disse må skiftes eller kontrolleres regelmessig. Utstyr som brukes sjelden, kan bli neglisjert slik at en motor ikke starter eller noe har rustet fast. Derfor er det spesielt viktig å vedlikeholde denne typen utstyr.

Tilgjengelighet

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

Oversikt og dokumentasjon

For at materiell og utstyr skal være tilgjengelig, er det viktig at KBO-enheten har oversikt over dette. Oversikten skal holdes oppdatert. Kravet gjelder ikke bare for reservemateriell og utstyr beregnet på kraftsystemet og anlegg, men også for driftskontrollsystemer med samband, relévern, driftsradio og andre nødvendige systemer.

KBO-enheter må gjennomføre systematisk kontroll og vedlikehold, og trene på bruk.

Sjøkabelberedskap i transmisjonsnett og regionalt distribusjonsnett

Alle eiere av sjøkabelanlegg i transmisjonsnett og regionalt distribusjonsnett skal ha tilgang på kompetanse, reparasjonsmaterieell, reservedeler og transportmidler slik at reparasjon eller utskifting av kabelanlegget i en ekstraordinær situasjon kan påbegynnes og utføres uten unødig opphold.



KBO-enheter må sørge for tilgang til følgende ressurser

- fartøy med nødvendig utstyr og mannskap
- biler for kabeltransport
- krankapasitet
- skjøtekompetanse
- reservelengder av kabel for innskjøting eller hele lengder for erstatning
- endemuffer, skjøtemuffer og overgangsmuffer for å dekke feil på mer enn en fase
- nødvendig reparasjonsmateriell, verktøy og utstyr
- festemateriell for landtak
- oversikt over reservedeler og reparasjonsutstyr og system for å holde dette i forsvarlig stand
- oppdaterte trasékart og inntegning av ankringsforbudssone i sjøkartet
- utstyr og kompetanse for feilsøking og feilstedlokalisering
- alternative planer for drift av nettet inntil anlegget igjen er fullt funksjonsdyktig
- sjekkliste for håndtering av kabelfeil for hvert enkelt kabelanlegg
- For hvert enkelt sjøkabelanlegg bør følgende dokumenteres og opplysningene være lett tilgjengelige
 - kontaktpersoner
 - handlingsplan ved kabelfeil
 - feilsøking og reparasjon
 - juridiske forhold og miljøspørsmål
 - informasjonshåndtering og varsling
 - avtaler og kontrakter om bistand
 - forsikringer
 - anleggsdata
 - reservedeler og reparasjonsutstyr
 - krav til reparasjonsfartøy og spesifisering for innleie
 - adresseliste over relevante leverandører, organisasjoner og myndigheter
 - oversikt over andre rør- og kabelinstallasjoner med eiere i området for kabelanlegget

Sjøkabelberedskap i lokalt distribusjonsnett

Viktige kabelanlegg uten reserver, dypt forlagte anlegg og lange sjøkabler bør ha samme reparasjonsberedskap som i regionalt distribusjonsnett.



Standarder

REN-blad 9301 Prosjektering av sjøkabelanlegg, se [REN-Renbladserie](#)
REN-blad 9305 Tilstandskontroll av sjøkabelanlegg - våt del
REN-blad 8032 Driftsmerking av 0,23-24 kV-Nett, pkt. 9.3 Sjøkabel
REN-blad 9307 Feilsøking sjøkabel ver 1.0

Beredskap for GIS-anlegg i sentral- og regionalt distribusjonsnett

Alle eiere av gassisolerte bryteranlegg i transmisjonsnettet og regionalt distribusjonsnett skal ha tilgang på kompetanse, reparasjonsmateriell, reservedeler og transportmidler slik at virksomheten kan utføre reparasjon eller utskifting av GIS-anlegget uten unødig opphold.



Virksomheter som eier GIS-anlegg, bør ha spesiell oppmerksomhet på tilgang til

- komplett reserve bryterfelt
- blindlokk for gassromseksjonering, mv.
- gass og påfyllingsutstyr
- kompetanse, ev. avtale med leverandøren av anlegget
- overspenningsavledere, høyspenningskabler, tilkoblinger / gjennomføringer, effektebrytere, skillebrytere, måletransformatorer, pakninger, lagre, mv.

I tillegg må virksomheten sørge for sikkerhetsutstyr og miljøhåndtering og opplæring i tråd med krav gitt av andre myndigheter.

Sikringstiltak og reservemateriell som det er gitt statstilskudd til etter tidligere bestemmelser

Gjennom årene er det gitt statstilskudd fra NVE til sikringstiltak og anskaffelse av reservemateriell etter søknad, med hjemmel i *forskrift om beredskap i kraftforsyningen utgitt 2003*, § 7-2, eller etter andre tidligere bestemmelser. Vilåårene som gjaldt da tilskuddet ble gitt, skal følges så lenge sikringstiltaket er relevant og reservemateriellet ikke har passert teknisk/økonomisk levetid.

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

Beredskapsmateriell som registreres hos REN Beredskap, kan særbehandles gjennom inntektsrammereguleringen. RME vurderer å endre ordningen med virkning fra 2021. [Kostnader ved investinger i beredskapsutstyr EØ-notat 3 2011](#)

4.5 Transport



§ 4-5 Transport

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

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

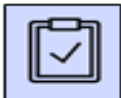
KBO-enhetenes transportmidler og private transportmidler tilhørende energiforsyningens personell som det er tjenstlig behov for, skal om mulig søkes fritatt for forberedt rekvirering til Forsvaret med videre.

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

Plan for transportberedskap

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

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



Planen for transportberedskap bør inneholde oversikt over

- kjøretøy og transportutstyr som enheten eier
- eventuelt eksternt (eksempelvis lånt, innleid) utstyr av beredskapsmessig betydning
- spesialutstyr, for eksempel helikopter, terrenggående kjøretøy, mobilkraner med mer som kan bidra til å bedre den regionale beredskapen
- personell som har nødvendige sertifikater for å føre kjøretøyene

- verksteder som kan brukes til reparasjon i en ekstraordinær situasjon
- tilgang til drivstoff
- eventuelle andre forhold enheten finner relevant

Planen for transportberedskap må være gjennomførbar. Det vil blant annet si at planen må inneholde beredskap for alternative transportruter ved uventede hendelser, der det er mulig.

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

Plan for transport av tunge og store komponenter

Alle komponenter som veier over 70 tonn eller har store ytre dimensjoner krever en egen plan. Både for reparasjon og utskifting er det nødvendig med en beredskapsplan for tungtransport. KBO-enheter skal derfor ha transportplaner som gir oversikt over hvordan store og viktige komponenter kan transporteres. Viktige komponenter må kunne repareres eller skiftes ut på kortest mulig tid. Dette reduserer ventetidene og konsekvensene ved havari. Det er transformatorer, generatorer, turbiner, ventiler og rør som er tyngst og har de største dimensjonene.



Oversikten bør inneholde

- type last
- vekt og største ytre dimensjoner
- transporttegning
- opp- og avlastingssted
- opplastingsplass og transportrute med angivelse av spesielle forhold
- oversikt over hvilket utstyr som skal brukes
- kjøretillatelse – beredskapsdispensasjon fra Statens vegvesen

Veier, broer, tunneller, jernbanelinjer og kaier kan være endret siden sist gang utstyret ble transportert, og det kan gi uforutsette begrensninger. Det er derfor viktig å avklare transportrutens begrensninger på forhånd og holde transportplanene oppdatert.

For å avklare hva som er *store ytre dimensjoner* må dette sees i forhold til de veiene som transporten skal gå på. Statens vegvesen har oversikter over transportbegrensninger på sin internettside Vekter, dimensjoner og spesialtransport på vegene – veglister. Totalvekt, akseltrykk, vogntoglengde, største høyde og transportbredde er viktig. Typiske komponenter som kan trenge spesialtransport og/eller tungtransport er transformatorer med transportvekt over 70 tonn, kuleventiler, turbinrør og store deler til vindkraftverk. Se også forskrift om bruk av kjøretøy kapittel 5 Vekt, dimensjoner.



Dispensasjon

Søk om dispensasjon på forhånd til Statens vegvesen!



Krysskoplinger til annet regelverk

[Vekter, dimensjoner og spesialtransport på vegene – veglister](#)

[Forskrift om bruk av kjøretøy](#) kapittel 5 Vekt, dimensjoner

Alle illustrasjoner med tillatelse fra Statnett:





Alle videoer med tillatelse fra Statnett:

[Transport På 144 hjul i svingen - YouTube](#)

[Transportplanlegging - YouTube](#)

[Transport Transformortransport Kvilldal - YouTube](#)

Drivstoff

I en krisesituasjon, for eksempel ved en rasjonering, vil bensinstasjonene kunne gå tomme for drivstoff før rasjonering settes i verk. KBO-enheten bør vurdere å ha eget drivstoffanlegg, eller inngå avtale om prioritet hos leverandør av drivstoff. Rasjonering av drivstoff kan innføres ved erklært beredskap og i krig og under knapphetssituasjoner i fredstid.

Forberedt rekvirering av sivile kjøretøyer

Forsvaret kan ved krigsberedskap rekvirere sivile kjøretøyer. Kjøretøyer som tilhører KBO-enheter, og private kjøretøyer til nøkkelpersonell som av tjenstlige grunner har behov for egen transport, er fritatt for forberedt rekvirering. Rekvirering er hjemlet i *lov om militære rekvisisjoner* §§ 1 og 5.

Forberedelse til rekvirering utføres etter *forskrift om militære rekvisisjoner*, §§ 11 og 37. Forskriften viser til *Håndbok for forberedt rekvirering av sivile kjøretøyer (TH 100-12)*, Forsvarets Logistikkorganisasjon, 1984, ved kode 911 og 934.

Forsvaret, i samarbeid med sivile beredskapsmyndigheter inklusiv DSB, definerer fritak fra rekvisisjon. I løpet av 2021 skal nasjonal ressursdatabase (NARDB) presenteres og innføres hos alle statsforvaltere for at sivilt beredskapsbehov og militært rekvisisjonsbehov samordnes, og for at eventuelle konflikter løses før et behov oppstår. NARDB skal ta hensyn til dette. Se [Forsvarets nettside om rekvisisjonsordningen](#).

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

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

Sivil transportberedskap

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



Krysskoplinger til annet regelverk

[Lov om militære rekvisisjoner \[Rekvisisjonsloven\]](#), §§ 1 og 5

[Forskrift om militære rekvisisjoner](#), §§ 11 og 37

Håndbok for forberedt rekvirering av sivile kjøretøyer (TH 100-12)

[Forskrift for sivil transportberedskap](#)

4.6 Nasjonal tungtransportberedskap



§ 4-5 Transport

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

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

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

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

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

Statnett SF disponerer transportmidler for tungtransport på jernbane, vei og til sjøs. Lufttransport må utføres med materiell som normalt ikke befinner seg i Norge.

Dekning av utgifter

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

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

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

Klargjøringstid

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

Ved *beredskap/krig* skal transportfunksjoner kunne iverksettes omgående når behov oppstår.

Mannskap som inngår i transportberedskapen, skal være fritatt for annen tjeneste i Totalforsvaret. Se § 3-5 om fritaksordninger.

4.7 Samband

§

§ 4-7 Samband

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

Ordforklaring

Samband	Et teknisk kommunikasjonssystem som understøtter informasjonsutveksling, tale eller data, mellom to eller flere parter.
---------	---

Hensikten med sambandsberedskap er å sørge for at nødvendig samband, enten det er i driftskontrollsystemet, i systemet for driftsradio, eller annet samband fungerer og at det repareres hvis det svikter. Krav til samband i driftskontrollsystemet og til driftsradio finner du i kapittel 7.

KBO-enheten skal ha samband som muliggjør kommunikasjon med personell som er viktig for å opprettholde energiforsyningen, også under ekstraordinære situasjoner. Dette gjelder

- nødvendig personell som må tilkalles
- montører og annet personell ute i felt
- personell i stasjoner
- personell ved andre kontorer i samme KBO-enhet
- KDS og andre KBO-enheter man har behov for å kommunisere med
- viktige eksterne leverandører, for eksempel entreprenører og leverandører av driftskontrollsystem
- myndigheter

Samme krav gjelder for kommunikasjon mellom tekniske systemer og komponenter for overvåking og styring av nettet. Ved svikt bør det finnes alternativer som raskt kan etableres.

KBO-enheter må for sine egne sambandssystemer også sørge for at

- enheten har nødvendig reparasjonsmaterieil og tilgang til reparasjonskompetanse for sitt sambandssystem
- det er tilstrekkelig nødstrøm til sambandssystemene

Mobilnettet har i varierende grad nødstrømkapasitet over mer enn to timer og kan slutte å virke ved strømbrytning. Det samme gjelder IP-basert telefonnett.

KBO-enheten bør bruke alle typer samband som er beskrevet i beredskapsplanen i daglig drift for å sikre at personellet som skal bruke sambandet, kjenner det. KBO-enheten må trene på bruken jevnlig.

Planlegging og dokumentasjon av sambandsberedskapen bør omfatte

- oversikt over de sambandsmidler enheten disponerer, for eksempel satellittelefoner, nødnett eller egne driftsradioer, og hvor utstyret befinner seg
- sambandsutstyrets viktigste egenskaper og funksjoner under ekstraordinære forhold
- oversikt over reserveløsninger
- oversikt over personell som kan bruke og reparere sambandet. Dette inkluderer blant annet personell i driftssentralen, ledelsen, reparasjonspersonell, personell som skal styre klassifiserte anlegg lokalt
- rutiner for bruk og opplæring
- vedlikeholdsrutiner, testing inklusive logg for eget utstyr
- avtaler med eksterne leverandører for vedlikehold, reparasjoner etc. (se også punkt under om eksterne leverandører)
- oversikt over digitale kommunikasjonssystemer, -tjenester og deres funksjon under strømbrytning. Eksempler er mobiltelefoni, tjenester for sms-varsling til kunder eller tjenester levert over internett, eksempelvis sosiale medier

Samband i ekstraordinære situasjoner

Talesamband er spesielt viktig når tiden er knapp og raske avklaringer og beslutninger må tas. KBO-enhetene må etablere sambandsberedskap med bruk av ulike kommunikasjonssystemer.

Kommunikasjonssystem, for eksempel egen driftsradio eller satellitt-telefoni, skal til enhver tid være klar til bruk.

Nødnett er et digitalt radiosamband driftet av Direktoratet for samfunnssikkerhet og beredskap. Nødnett kan benyttes for å oppfylle kravet i denne paragrafen i de områdene hvor Nødnett har tilfredsstillende dekning. Dersom ikke nødnettet eller eget mobilt radionett er tilgjengelig, skal sambandsberedskapen ivaretas på annen måte, som for eksempel ved satellittelefon, mobiltelefoni levert av ulike leverandører, jaktradio eller annet.

Eksterne leverandører av sambandstjenester – avtaler

Ved kjøp av sambands- og kommunikasjonssystemer bør leveransepålitelighet og service for tjenesten kontraktfestes.

For nærmere krav til samband i driftskontrollsystemer, se kapittel 7 og for mobile radionett - driftsradio, se § 7-17.



Forhold som bør avklares og fastsettes i avtale

- vilkår ved mobilabonnement (prioritet)
- dekningsområde og oppetid for tjenesten
- nødstrøm og levetid etter strømbrudd, ev oversikt over tjenestebortfall ved strømbrudd
- apparat til apparat kommunikasjon og avhengighet av sentraliserte kommunikasjonstjenester
- Mulighet for å prioritere brukere eller samtaler
- gruppesamtaler
- kryptert samband
- dataoverføringskapasitet eller båndbredde i henhold til behov
- supportgaranti med tidsfrist



Nyttig informasjon

[Nødnett hjemmeside](#)

[Dekningskart for ulike mobiltjenester](#)

[Nasjonal kommunikasjonsmyndighet NKOM](#)

[Prioritetsabonnementer i mobilnett](#)



Krysskoplinger til annet regelverk

§ 2-10 Internkontroll

§ 5-1 Sikringsplikt

Vedlegg til kapittel 5

§ 7-17 Mobile radionett - driftsradio

Innhold

5	KLASSIFISERING OG SIKRINGSTILTAK	2
5.1	SIKRINGSPLIKT	2
5.1.1	KONTROLL OG VEDLIKEHOLD AV SIKRINGSTILTAK	4
5.1.2	ADGANGSKONTROLL FOR UVEDKOMMENDE	4
5.1.3	ANLEGGENE SKAL HOLDES I STAND OG VIRKE ETTER HENSIKTEN	7
5.1.4	SÆRLIG HENSYN TIL EKSTRAORDINÆRE FORHOLD	7
5.2	KLASSER	8
5.2.1	HENSIKTEN MED OG BAKGRUNNEN FOR KLASSIFISERINGEN	9
5.2.2	ANLEGG SOM INNGÅR I KLASSIFISERINGEN	10
5.2.3	MER OM KLASSIFISERING AV DRIFTSKONTROLLSYSTEM	11
5.2.4	KLASSIFISERING AV TRANSFORMATORSTASJON FOR OVERFØRING AV VINDKRAFT	13
5.2.5	KLASSIFISERING AV FJERNVARMEANLEGG	13
5.2.6	ANLEGG SOM IKKE INNGÅR I KLASSIFISERINGEN	14
5.2.7	HVORDAN KLASSIFISERE ANLEGG SOM HAR FLERE FUNKSJONER OG EIERE.....	15
5.2.8	KLASSIFISERING ETTER YTELSE ER FASTSATT PÅ GRUNNLAG AV MERKEYTelser.	16
5.2.9	KLASSIFISERING ETTER SPENNINGSNIVÅ (kV) I KRAFTLEDNINGER.....	17
5.3	SIKRING AV KLASSIFISERTE ANLEGG	18
5.4, 5.5 OG 5.6	SIKRINGSTILTAK FOR KLASSE 1, 2 OG 3	20
5.4-, 5.5- OG 5.6- 1	SIKRINGSTILTAKENES FORMÅL	20
5.4-, 5.5- OG 5.6- 2	FUNKSJONSBASERTE KRAV TIL SIKRINGSTILTAK	21
5.4-, 5.5- OG 5.6- 3	SÆRSKILTE KRAV I VEDLEGG 1, 2 OG 3.FOR SIKRING AV KLASSIFISERT ANLEGG	21
5.4-, 5.5- OG 5.6- 4	RELEVANTE NORMER OG STANDARDER	22
5.7	VEDTAK OM SIKRING ELLER KLASSE	23
5.8	VURDERING	23
5.8.1	VURDERING AV RISIKO VED BYGGING, ENDRING ELLER UTVIDELSE AV ANLEGG.....	23
5.9	MELDEPLIKT OM SIKRINGSTILTAK	25
	HENSIKTEN MED MELDEPLIKTEN.....	25
5.10	VAKTHOLD	26
	BEHOV FOR EKSTRA VAKTHOLD VED UTVALGTE KRAFTFORSYNINGSANLEGG	26
	PLANLEGGING OG GJENNOMFØRING AV VAKTHOLD.....	27
	TILRETTELEGGE FOR ØVELSER VED HØYSPENNINGSANLEGG	27
	ADGANG FOR POLITI OG FORSVAR	27
5.11	RESTRIKSJONER FOR ADGANG TIL STEDER OG OMRÅDER.....	28
5.12	FORHOLDET TIL ANNET REGELVERK OG STANDARDER	30

5 Klassifisering og sikringstiltak

Dette kapitlet handler om sikring og klassifisering av anlegg og system som er eller kan bli av vesentlig betydning for kraftforsyningen, dvs. forsyning av elektrisitet og fjernvarme.

Sikringsplikt for slike anlegg og systemer, er fastsatt i *energiloven* § 9-2 (beredskapstiltak).



Energiloven § 9-2 første ledd:

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

Virksomheten skal planlegge og innarbeide relevante sikringstiltak på et tidlig tidspunkt i planleggingsprosessen.



Merk at vedlegg til kapittel 5 er også forskriftskrav. Se eget kapittel for vedleggene. Kapitlet har en annen struktur på både forskriftstekst og veiledningstekst enn de andre kapitlene i forskriften.

5.1 Sikringsplikt



§ 5-1. Sikringsplikt

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

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

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

Det skal særlig tas hensyn til ekstraordinære forhold som:

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

Ordforklaring

Adgang	Blir i denne forskriften brukt om fysisk adgang til anlegg og områder
Tilgang	Blir i denne forskriften brukt om tilgang på personell (kap. 4), materiell (kap 4 og 5), kraftsensitiv informasjon (kap 6) og til driftskontrollsystemer (kap 7). Blir i dette kapitlet brukt om tilgang til reserver.

Virksomheter må sørge for å etablere et grunnleggende av sikringsnivå og motvirke uønskede hendelser og handlinger ved alle anlegg, bygg, systemer, ressurser, materiell, utstyr og annet av betydning for kraftforsyningen. Dette gjøres på bakgrunn av risikovurdering, se § 2-3 (risikovurdering) og § 5-8 (vurdering), som tar hensyn til stedlige forhold og risiko. Det bør være en riktig balanse mellom sikringstiltakene, og for klassifiserte anlegg er dette et krav, se § 5-3 og §§ 5-4 til 5-6 inkludert vedlegg om sikringstiltak for klasse 1 til 3, om særlige krav til sikring av anlegg. Se også § 2-10 (internkontrollsystem).

Sikringsplikten gjelder for alle som eier eller driver energianlegg mv. som er eller kan bli av vesentlig betydning for kraftforsyningen, og omfatter både anlegg, bygg og ressurser etter kapittel 4 om ressurser og reparasjonsberedskap.

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

Sikringsplikten gjelder også for eiere av anlegg som ikke er konsesjonspliktige, som for eksempel driftskontroll- og sambandsanlegg, og ressurser som for eksempel lagerbygg og reservemateriell. Dersom slike anlegg drives av en annen virksomhet, må eieren avtale at denne også får ansvar for sikringsplikten.



Eksempler på balanse mellom sikringstiltak

En solid port inn til et adgangskontrollert område får begrenset effekt dersom gjerdet rundt området har for dårlig kvalitet, eller er mangelfullt vedlikeholdt.

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

Ventilasjons-, tak-, kjeller-, kabelkanal-luker mv. må ha samme sikringsnivå som dører, porter og vinduer.

5.1.1 Kontroll og vedlikehold av sikringstiltak

For å kunne føre tilstrekkelig kontroll og vedlikehold med sikringstiltakene, må virksomheten ha oversikt over hvilke sikringstiltak som er pålagt og gjennomført.

Virksomheten må sørge for at følgende blir gjennomført og dokumentert:

- Føre en oppdatert oversikt over sikringstiltakene
- Ha en oppdatert beredskapsplan for bruken av tiltakene, når tiltakene skal settes i verk,
- Ha en plan for hvem som skal gjøre hva og hvilke ressurser det er behov for (personell, verktøy, maskiner, med mer)
- Innarbeide kontroll og vedlikehold av sikringstiltakene i virksomhetens vedlikeholdssystem/kvalitetssystem, som sikrer en fornuftig frekvens på kontrollene
- Teste sikringstiltakene jevnlig for å se om de fungerer etter hensikten
- Sørge for at defekte tiltak erstattes eller repareres
- Andre nødvendige tiltak for at sikringstiltakene fungerer hensiktsmessig

Materiell og utstyr til sikringstiltak som ikke er i daglig bruk, må oppbevares hensiktsmessig, slik at det ikke blir ødelagt. Materiellet og utstyret må være tilgjengelige og håndterbare, slik at de raskt kan tas i bruk ved behov.



Eksempel: Kraftstasjon med rulleport ytterst i adkomsttunnelen

Sløvika kraftstasjon er i klasse 2 og har en rulleport ytterst i adkomsttunnelen. Innenfor rulleporten er den gamle kraftverksporten i stål. Denne er så tung at det er nesten umulig for én person å åpne og lukke den. Ventilasjonsluften som strømmer gjennom tunnelen, gjør det ekstra tungt når stasjonen er i drift. Derfor har virksomheten sluttet å bruke den gamle porten og lar den alltid stå åpen. Adgangskontrollen er ivarettatt med rulleporten, men kravet til sikring av anlegg i klasse 2 var ikke oppfylt!

Porten måtte derfor vedlikeholdes slik at den kunne brukes og kravet til sikring ble oppfylt.

Beredskapskoordinator vil vurdere vedlikeholdet av sikringstiltak i stasjonen. Stålporten er ett av sikringstiltakene. Porten er verken vedlikeholdt eller klar til bruk. Rulleporten er for svak til å være et fullverdig sikringstiltak. I samråd med driftsleder finner beredskapskoordinator ut at de må gjøre noe med den gamle porten. De smører opp hengslene og låseinnretningen. Etter dette er det mulig å åpne og stenge porten, men ved full ventilasjonsluftgjennomgang er det svært utfordrende. De beslutter å vurdere hydrauliske sylindere til porten. I tillegg fastsetter de en rutine som sier at kraftverksporten skal være lukket når det ikke er folk i stasjonen.

5.1.2 Adgangskontroll for uvedkommende

Virksomheten må sikre mot fysisk adgang for uvedkommende i anlegg og områder. Krav til sikring mot tilgang til logiske systemer er gitt i kapittel 6 og 7. Andre relevante krav er gitt sjekklisten nedenfor.

Kravet innebærer at virksomheten må ha kontroll over hvem som ut fra et tjenstlig behov skal ha selvstendig fysisk adgang til anlegg og områder. Adgangskontrollen omfatter også hvem som kan gis

adgang i følge med, eller under oppsyn av en person som har selvstendig adgang. For alle andre skal området være effektivt avstengt.

Figur 1 som viser prinsipp for område, skall og soner med angitt nivå for adgangskontroll av disse.

Utendørs område for allmenn ferdsel



Figur 1 Prinsipp for område-, skall- og sonesikring mot adgang.

Sjekkliste: Adgangskontroll skal som minimum gjelde for

Driftssentraler, inkludert reservesentraler, sambandsanlegg og rom med tilhørende utrustning for driftskontroll og lokalkontroll i klassifiserte anlegg

Beredskapsrom og rom med IKT-utstyr av betydning for beredskap, drift og sikkerhet

Bygg og områder med klassifiserte kraftforsyningsanlegg

Bygg for ledelse, drift og andre vesentlige ressurser for beredskap, drift, sikkerhet og gjenoppretting

Lagerområder ute og inne for materiell, kjøretøy og annet av vesentlig betydning for beredskap, drift, sikkerhet og gjenoppretting



Virksomheten kan etablere adgangskontroll med kombinasjoner av avlåsning, vakthold, overvåking, registrering og/eller ved bruk av andre tekniske løsninger. Det må være balanse mellom adgangskontroll og andre fysiske sikringstiltak.

Virksomheten må innarbeide en rutine for å kontrollere at porter, dører og vinduer fungerer etter hensikten, dvs. både at de lar seg lukke og låse og at de normalt holdes lukket og låst. Virksomheten må ha full kontroll med tilgangsrettigheter for nøkkelsystemer. Alminnelige låsesystemer er sårbare for at nøkler mistes, og virksomheten må ha rutiner for administrering, slik at nøkler på avveie oppdages og at relevante tiltak blir gjennomført. Virksomheten bør bruke adgangskontrollsystemer som kan logge aktivitet. Slike logger bør gjennomgås jevnlig for å avdekke hendelser av sikkerhetsmessig betydning

I anleggsfaser må virksomheten etablere adgangskontroll senest fra det tidspunkt bygge- eller installasjonsarbeidet starter. Alle faste adgangsberechtigede må utstyres med adgangskort. Tilfeldige arbeidstakere, leverandører, besøkende og liknende må gis tidsbegrensede adgangskort. Kjøretøyer må være registrert og ha parkeringstillatelse.

Det er viktig å deaktivere adganger og tillatelser ved avslutning av anleggsfasen.



NVE anbefaler å holde kontroll (loggføring) med egne autoriserte ansattes gange og opphold inne i et anlegg, selv om denne forskriften ikke krever det. For anlegg med adgangstreksjoner etter § 5-11 er det krav om å bekrefte identitet for personer på besøk og det skal være protokollføring av besøkene.

Sjekkliste: Andre relevante krav til adgangskontroll

§ 5-4 Sikringstiltak for klasse 1, vedlegg 1.1.1 og 1.1.3

§ 5-5 Sikringstiltak for klasse 2, vedlegg 2.2.3, 2.3.1, 2.3.5 og 2.4.1.3

§ 5-6 Sikringstiltak for klasse 3, vedlegg 3.2.5, 3.3.1, 3.3.4 og 3.4.1.3

§ 5-11 Restriksjoner for adgang til steder og områder



Særlig om adgangskontroll ved driftssentraler mv: Driftssentraler med tilhørende utrustning omfatter: Driftssentraler, sambandsanlegg og øvrige anlegg og rom med komponenter som ivaretar driftskontrollfunksjoner eller kan gi fysisk eller elektronisk adgang til slike.

- Alle deler av bygningen eller anlegget der driftssentralen, operatørrom, prosessanlegg, viktige IT- og sambandsanlegg og nødstrøm er plassert
- Alle rom der driftskontroll kan utøves, som f.eks. styring av koblinger og overvåking av tilstand i anleggene

Slike steder skal være egne adgangskontrollerte sikkerhetssoner for å hindre at uvedkommende får adgang. Virksomheten må holde disse rommene avlåst for alle som ikke skal ha selvstendig adgang. Personer kan få selvstendig adgang gjennom autorisering. Øvrige personer må ledsages av personer som har gyldig autorisasjon.

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

5.1.3 Anleggene skal holdes i stand og virke etter hensikten

Tredje ledd understreker at krav til beredskap ikke bare gjelder forberedte og ytre sikringstiltak, men også krav til at anleggene fungerer som de skal i en ekstraordinær situasjon når behovet er størst. Kravet framgår også av plikter for konsesjonær, se *energilovforskriften* [§ 3 – 5 c og 5-3 c](#).

For et anlegg som blir rammet av en uønsket hendelse eller handling, skal sikringstiltakene være innrettet slik at anlegget likevel fungerer så godt som mulig. Forbyggende tiltak, redundans i anlegg og system og evne til å håndtere og gjenopprette anleggets funksjon, er viktige deler av beredskapen. Sikringsplikten må ses i sammenheng med disse elementene.

5.1.4 Særlig hensyn til ekstraordinære forhold

Listen over ekstraordinære forhold i fjerde ledd er ikke uttømmende. Tiltakene skal også ta hensyn til tilsiktede uønskede handlinger og forberedelser til slike. I den sammenheng kan nåværende og tidligere ansatte utgjøre en risiko for virksomheten i form av ondsinnete handlinger eller trusler.

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



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 2-3 Risikovurdering](#)
- [§ 2-10 Internkontrollsystem](#)
- [§ 5-4 Sikringstiltak for klasse 1](#)
- [§ 5-5 Sikringstiltak for klasse 2](#)
- [§ 5-6 Sikringstiltak for klasse 3](#)
- [§ 5-8 Vurdering](#)
- [§ 5-11 Restriksjoner for adgang til steder og områder](#)

Kopling til annet regelverk

- [Energilovforskriften](#)

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

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

Klasse 1 omfatter:

- a. Kraftstasjon med samlet installert generatorytelse på minst 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 nettførmål, 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*

5.2.1 Hensikten med og bakgrunnen for klassifiseringen

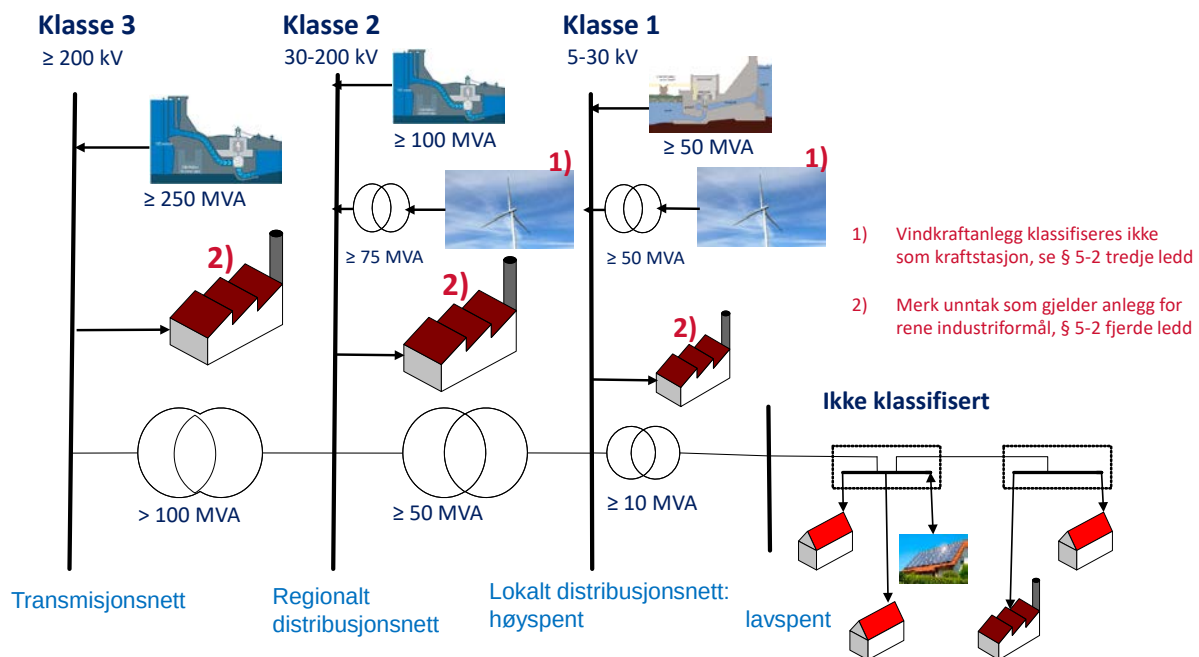
Klassifiseringen er grunnlaget for å fastsette differensierte krav til sikringstiltak og -nivå for ulike kraftforsyningsanlegg ut fra deres betydning. Anlegg og systemer klassifiseres etter kriteriene i forskriften.



Se også veiledningen til § 8-9 om forholdet til eldre vedtak om klassifisering og overgangsregler.

Klasse for kraftforsyningsanlegg er gitt av de ytelses- og spenningskriteriene som er angitt i denne bestemmelsen. Bestemmelsen gir et logisk og forutsigbart system for å differensiere krav til sikringsnivå i tre klasser etter hvilken betydning de ulike anleggene har for kraftforsyningen.

Figur 2 viser prinsipp for hvordan klassifiseringen er fastsatt i et logisk system for klassifisering etter anleggenes ytelse og nettnivå. Transmisjonsnett er i hovedsak klasse 3, regionalt distribusjonsnett klasse 2 og lokalt distribusjonsnett i klasse 1. For kraftstasjoner og fjernvarmeanlegg er kriteriet samlet installert ytelse (merkeskilt).



Figur 2 Prinsippskisse for klassifisering etter § 5-2. (Fjernvarmeanlegg er ikke med på skissen)

Eksempler på anlegg med annen klasse enn det som kommer frem av bestemmelsen:

Eksempel 1: Transmisjonsnett (kl. 3) på 132 kV kan enkelte steder være svakere fysisk dimensjonert enn deler av 132 kV regionalt distribusjonsnett (kl. 2) i andre områder.

Eksempel 2: En middels stor kraftstasjon som anses som en viktig stasjon for et lokalt forsyningsområde kan ha høyere klasse enn ytelsen skulle tilsi, fordi området ikke har annen kraftproduksjon, eller fordi nettet inn til om området har lav overføringskapasitet.

5.2.2 Anlegg som inngår i klassifiseringen

Transformatorstasjoner: Sikring i henhold til klasse omfatter hele anlegget med alle elektrotekniske, mekaniske og bygningsmessige installasjoner. Lokalt kontrollanlegg, koblingsanlegg, muffeanlegg, tilhørende anleggsdeler og annen utrustning er inkludert.

Kraftstasjoner: Sikring i henhold til klasse omfatter hele anlegget med alle elektrotekniske, mekaniske og bygningsmessige installasjoner. Lokalt kontrollanlegg, koblingsanlegg, muffeanlegg, tilhørende anleggsdeler og annen utrustning er inkludert.

For vannkraftstasjoner omfattes den del av vannveien som har direkte betydning for drift og sikring av stasjonen. Dammer og vassdragsreguleringsanlegg av vesentlig betydning for kraftproduksjon, følger sikringsplikten for kraftstasjonens klasse. Kraftstasjoner med en samlet ytelse på mindre enn 50 MVA er

ikke lenger klassifisert, se § 8 -9. For kraftstasjoner bygget i fjell utgjør fjellet en vesentlig del av sikringen. Kraftstasjoner på minst 250 MVA som ikke er plassert i fjell, er i klasse 2.

Selvstendige koblingsstasjoner: Sikring i henhold til klasse omfatter samleskinner, brytere og felt for avganger til kraftledninger. Med selvstendig koblingsstasjon, menes koblingsanlegg som ikke tilhører en kraftstasjon eller transformatorstasjon. I de tilfeller der koblingsanlegg funksjonelt tilhører en kraft- eller transformatorstasjon, blir koblingsanlegget regnet som en del av den stasjonen det tilhører og får klasse etter denne. Med funksjonelt tilhørende menes at anlegget er direkte koblet til kraft- eller transformatorstasjonen og at koblingsanlegget er en viktig del av videre forsyning. I de tilfeller hvor koblingsanlegget er viktigst, skal dette klassifiseres som selvstendig koblingsstasjon, og gis klasse etter spenningsnivå.

Driftskontrollsystemer: Se definisjon av driftskontrollsystem i § 7-1. Lokalkontrollanlegg og annet som funksjonelt er en del av en kraft-, transformator-, koblings- eller omformerstasjon, klassifiseres etter vedkommende stasjons klasse. Dersom lokalkontrollanlegget har komponenter og anleggsdeler som har betydning for hele eller deler av driftskontrollsystemet som styrer anlegg utenfor det lokale anlegget, klassifiseres disse etter driftskontrollsystemets klasse.

Omformerstasjon: Sikring i henhold til klasse omfatter like-/vekselretting med transformering, koblingsanlegg og annen utrustning, og omfatter større (samlet ytelse på minst 10 MVA) AC/DC anlegg for HVDC kabler og for jernbanedrift. Det er kontinuerlig ytelse som angitt på merkeskiltet, og ikke kortvarig ytelse, som legges til grunn. NVE har ikke utarbeidet spesifikke sikringskrav til omformerstasjoner, men bestemmelsene om sikring av transformatorstasjoner, koblingsanlegg mv. brukes så langt disse passer. Det stilles normalt ikke særlige krav til fysisk beskyttelse av ventilhaller e.l. Her gir bestemmelsene i § 5-7 hjemmel til å treffe tilpassede enkeltvedtak om sikringstiltak.

Sambandsanlegg regnes normalt som en del av det driftskontrollsystemet det betjener, og skal sikres i henhold til driftskontrollsystemets klasse. Sambandsanlegg som bare benyttes til driftsradio, klassifiseres ikke.

Kraftledninger: Sikring i henhold til klasse omfatter alle ledninger som kan overføre elektrisk kraft (vekselstrøm eller likestrøm), både luftledning og kabel (sjø og land) med tilhørende elektriske og bygningstekniske installasjoner, herunder muffeanlegg, brytere og T-avgreininger mv, når dette ikke er del av et annet anlegg. Den omfatter også den fysiske ledningstraseen så langt denne har beredskapsmessig betydning for sikring, drift og gjenoppretting. Klassifiseringen omfatter kraftledninger på minst 5 kV i lokalt fordelingsnett, men ikke de tilhørende nettstasjonene.

Fjernvarmeanlegg: Sikring i henhold til klasse, omfatter hele varmesentralen med alle bygninger, teknisk utrustning og tilhørende bygningstekniske konstruksjoner.

5.2.3 Mer om klassifisering av driftskontrollsystem

Driftskontrollsystemer i klasse 2 og 3 klassifiseres etter den høyeste klassen gitt av enten befolkningsstørrelse eller antall klassifiserte anlegg som styres. Befolkningsstørrelsen er av spesiell betydning for nettvirksomheter. Kraftprodusenter har ingen befolkningsstørrelse å forholde seg til. For disse vil det altså være klassen til de anleggene som styres av driftskontrollsystemet som er av betydning for klassifiseringen. Styrer driftskontrollsystemet flere anlegg i klasse 2, er driftskontrollsystemet også klassifisert i klasse 2. Det samme gjelder for klasse 3.

Et driftskontrollsystem plasseres i samme klasse som anlegg i klasse 2 eller 3 som det styrer, når antall anlegg er minst tre. Dette gjelder både for nettanlegg og produksjonsanlegg. Når flere virksomheter

samarbeider om et driftskontrollsystem, må den samlede befolkning og det samlede antall stasjoner legges til grunn. Se tabell 1 og 2 nedenfor.



NVEs forvaltningspraksis hittil er at med «flere anlegg» i åttende ledd bokstav h og niende ledd bokstav e regner vi minst tre. (se eksempel nedenfor)



Eksempel:

Klassifisering av driftskontrollsystem for liten virksomhet som har to klasse 2 stasjoner

Mini Nett AS er en liten nettvirksomhet som forsyner elektrisitet til en befolkning på ca. ti tusen. Virksomheten har en driftssentral som er satt i klasse 1 etter vedtak fra NVE. Vedtaket er gitt etter 2003, men før 2013, og står ved lag inntil NVE endrer eller opphever vedtaket, i henhold til § 8-9 annet ledd.

Virksomheten har to transformatorstasjoner i klasse 2. Den ene stasjonen er ombygget etter 2003 men før 2013 og har fått økt samlet transformatorytelse over 50 MVA. Det er ikke gitt noe enkeltvedtak om klasse for stasjonen. Stasjonen havne automatisk i klasse 2 i henhold til § 8-9 annet ledd.

Så lenge Mini Nett AS ikke har flere enn to anlegg i klasse 2 (§ 5-2 annet ledd bokstav a til g), endrer ikke NVEs tidligere forvaltningspraksis og driftskontrollsystemet fortsetter å være i klasse 1.

Tabell 1: Driftskontrollsystem for nettvirksomhet

Befolkning	Antall anlegg	Driftskontrollsystem
Inntil 50 000	Ikke krav til antall klassifiserte anlegg	Klasse 1
Inntil 50 000	Minst 3 klassifiserte (klasse 2)	Klasse 2
Inntil 50 000	Minst 3 klassifiserte (klasse 3)	Klasse 3
50 000 og inntil 250 000	2 klassifiserte	Klasse 2
50 000 og inntil 250 000	Minst 3 klassifiserte (klasse 3)	Klasse 3
Minst 250 000	2 klassifiserte (klasse 1-3)	Klasse 3
Minst 250 000	Minst 3 klassifiserte (klasse 3)	Klasse 3

Tabell 2: Driftskontrollsystem for fjernvarmevirksomhet

Befolkning	Antall anlegg	Driftskontrollsystem
Inntil 50 000	1-2 klassifiserte (klasse 1-2)	Klasse 1
Inntil 50 000	Minst 3 klassifiserte (klasse 2)	Klasse 2
50 000 og inntil 250 000	1-2 klassifiserte (klasse 1-2)	Klasse 2
50 000 og inntil 250 000	Minst 3 klassifiserte (klasse 1-2)	Klasse 2
Minst 250 000	1-2 klassifiserte (klasse 1-2)	Klasse 2
Minst 250 000	Minst 3 klassifiserte (klasse 2)	Klasse 2

Tabell 3: Driftskontrollsystem for vannkraft og vindkraft

Antall anlegg	Driftskontrollsystem
Ingen klassifiserte	Uklassifisert (ikke KBO)
1-2 klassifiserte (klasse 1-2-3)	Klasse 1
Minst 3 klassifiserte (klasse 1)	Klasse 1
Minst 3 klassifiserte (klasse 2)	Klasse 2
Minst 3 klassifiserte (klasse 3)	Klasse 3

5.2.4 Klassifisering av transformatorstasjon for overføring av vindkraft

Vindkraftanlegg med vindturbiner og lokalkontrollanlegg for disse klassifiseres ikke. Det er kun transformatorstasjonen for overføring av produsert vindkraft til regionalt- eller lokalt distribusjonsnett som klassifiseres. Dersom hovedtransformatorenes samlede ytelse er mindre enn 75 MVA klassifiseres ikke stasjonen. Samlet hovedtransformatorytelse f.o.m. 75 MVA til 500 MVA er klasse 1, mens ytelse på minst 500 MVA, er klasse 2.

Dersom transformatorstasjonen til vindkraftanlegget transformerer til nettformål (lokal forsyning) i tillegg til å overføre produsert vindkraft til regionalt eller lokalt distribusjonsnett, vil stasjonen klassifiseres som nettransformator iht. bokstav b i hhv første (minst 10 MVA i klasse 1), annet (minst 50 MVA i kl.2) eller tredje ledd (over 100 MVA i kl. 3.)

5.2.5 Klassifisering av fjernvarmeanlegg

Varmesentraler med en samlet ytelse på mindre enn 50 MW er uklassifisert. Når varmesentralen er minst 50 MW klassifiseres den i klasse 1. Varmesentraler med samlet ytelse minst 150 MW er i klasse 2. Ingen fjernvarmeanlegg er klassifisert i klasse 3. Det er ikke mulig å sikre en varmesentral etter kravene til klasse 3 hvis den ikke er bygget i fjell, men NVE kan stille tilleggskrav til særlig kritiske varmesentraler. Samlet ytelse er basert på kjelenes merkeeffekt og eksternt tilført varme, eksempelvis fra et forbrenningsanlegg.

5.2.6 Anlegg som ikke inngår i klassifiseringen

Anlegg for rene industriformål: Anlegg som for eksempel transformatorer, omformere (likerettere), kraftledning, samt fjernvarmeanlegg som eies av virksomheten selv for egne formål og som ikke i vesentlig grad forsyner andre sluttbrukere, klassifiseres ikke etter denne bestemmelsen, men kan bli klassifisert ved enkeltvedtak etter § 5-7. Det er sluttbrukergruppene innen industri (iht. FASIT kravspesifikasjon) som legges til grunn ved bruk av termen *rene industriformål*, se Tabell 4. Sluttbrukergruppene er basert på standard SN2007 for næringsgruppering (ref Statistisk Sentralbyrå).

Tabell 4: Sluttbrukergrupper innen industri som faller inn under anlegg som ikke inngår i klassifiseringen, dersom forsyningen til anlegget er til rene industriformål

Sluttbruker-gruppe nr.	Sluttbrukergruppenavn	Næringskode-standard SN2007	Kundegruppe for KILE iht. kontrollforskriften § 9-2
2	Bergverksdrift	05+07-09, unntatt 09.1	Industri
3	Utvinning av råolje og naturgass	06	Eldrevne prosesser
4	Tjenester tilknyttet utvinning av råolje og naturgass	09.1	Industri
5	Produksjon av papirmasse, papir og papp	17.1	Eldrevne prosesser
6	Produksjon av kjemiske råvarer	20.1	Eldrevne prosesser
7	Produksjon av jern og stål	24.101	Eldrevne prosesser
8	Produksjon av ferrolegeringer	24.102	Eldrevne prosesser
9	Produksjon av primæraluminium	24.421	Eldrevne prosesser
10	Produksjon av andre ikke-jernholdige metaller	24.4, unntatt 24.421	Eldrevne prosesser
11	Næringsmiddelindustri	10+11+12	Industri
12	Raffineri	19,2	Eldrevne prosesser
13	Annen industri		Industri

Dammer og vassdragsreguleringsanlegg som ikke forsyner en klassifisert kraftstasjon klassifiseres etter damssikkerhetsforskriften.

Vindkraftanlegg Vindkraftanlegg med vindturbiner og lokalkontrollanlegg for disse klassifiseres ikke.

Omformerstasjoner for jernbane og sporveisdrift på mindre enn 10 MVA klassifiseres ikke.

Midlertidig anlegg Omfatter anlegg hvor det er planer om nært forstående om- og utbygginger. Dette omfatter også anlegg der det er behov for å etablere midlertidige løsninger i forbindelse med nett- og kraftutbygginger, for eksempel midlertidige tilkoblinger eller transformering mellom eksisterende og framtidig spenning. I slike tilfeller kan NVE for et avgrenset tidsrom akseptere at slike anlegg eller anleggsdeler ikke sikres iht. klasse. Øvre grense for varighet av midlertidige løsninger er anslått til fem år.

NVE forutsetter at det foreligger konkrete planer for utbygging eller oppgraderinger. Tvilstilfeller avgjøres av NVE. Etter byggefasen og når anlegget / anleggsdelen kan anses for permanent, skal virksomheten uoppfordret sikre anlegget etter riktig klasse.



Eksempel: midlertidige anlegg

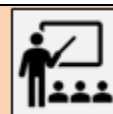
Hvis transformator med tilhørende arrangementer inngår i midlertidige løsninger i forbindelse med konkrete planer for nettutvikling med ombygging fra et spenningsnivå til et annet, kan transformatoren også unntas fra å inngå i ytelsesgrunnlaget for klassifiseringen. Sikringstiltakene ved transformatoren kan utføres tilsvarende mer moderat. NVE kan for eksempel akseptere at virksomheten ikke etablerer transformatorcelle der transformatoren ikke blir en del av det fremtidige permanente anlegget.

Det må være en konkret plan for tilbakeføring til endelig anlegg, og det kan være nødvendig med midlertidige sikringstiltak, som f.eks vakthold.

5.2.7 Hvordan klassifisere anlegg som har flere funksjoner og eiere

Enkelte kraftforsyningsanlegg ivaretar ulike funksjoner i kraftsystemet (produksjon, transmisjonsnett, regionalt distribusjonsnett, osv.) og ulike deler av anlegget kan være fordelt på flere eiere. Hvis anleggets funksjoner og eiere har naturlig sammenfall med anleggets fysiske og elektriske inndeling, kan anlegget deles opp slik at ulike deler får ulik klasse. Dette forutsetter en vesentlig forskjell i de ulike anleggenes betydning og må være i overensstemmelse med kriteriene for klassifisering i denne bestemmelsen.

Andre steder vil betydning og risikobilde tilsi at anlegget som helhet sikres etter den klassen som er dekkende for viktigste funksjon(er) eller summen av ulike funksjoner. Sekundære deler av anlegget kan likevel sikres etter lavere klasse, hvis kravet i § 5-3 om at risikoen skal bli minst mulig er oppnådd og en risikovurdering iht. § 2-3 kan begrunne det.



Eksempel: Anlegg med flere funksjoner og eiere

I en 420 kV selvstendig koblingsstasjon i klasse 3 skal det settes inn en 40 MVA transformator for lokal forsyning. Dette anlegget blir ikke automatisk en transformatorstasjon i klasse 1. Hele anlegget må sikres etter viktigste funksjon, dvs. 420 kV-anlegget. Eventuelt, hvis transformatoren funksjonelt og fysisk kan skilles fra øvrig anlegg, kan anlegget betraktes som én koblingsstasjon i klasse 3 og én transformatorstasjon i klasse 1. Dette forutsetter at en feil, et havari eller en villet ødeleggelse av transformatorstasjonen ikke får konsekvenser for koblingsstasjonen.

Hvis det ikke er naturlig å dele opp et anlegg med flere funksjoner i flere klasser, skal den klassen som er utløst på grunn av den viktigste funksjonen, være bestemmende for hele anleggets klasse.



Eksempel:

Industribedrift med en stor selvstendig koblingsstasjon, stor transformatorytelse, der en liten andel av ytelsen går til alminnelig forbruk

En stor kraftkrevende industribedrift har samlet transformatorytelse på 200 MVA. En liten andel av denne ytelsen (ca. 12 MVA) er til alminnelig forbruk til ca. 4000 innbyggere i lokalsamfunnet, mens resten er til industriformål. Av historiske og praktiske årsaker er uttak av kraft til industrien og til lokal områdekonsesjonær tilknyttet de samme transformatorene. Det er ikke fysisk mulig å skille mellom forsyning til industriformål og til alminnelig forbruk. Anlegget må derfor klassifiseres. NVE har lagt befolkningsmengde, ikke total transformatorytelse, til grunn i et enkeltvedtak iht. § 5-7, og anlegget er gitt klasse 1.

Industribedriften har i tillegg en stor koblingsstasjon med 20 bryterfelt som mater kraft til både industrien, lokal forsyning og til regionale distribusjonsnettet i området. Koblingsstasjonen er i eget bygg som er fysisk uavhengig av sikringstiltakene til transformatorstasjonen. På grunn av at koblingsstasjonen er viktig både for det regionale og det lokale distribusjonsnettet har NVE i et enkeltvedtak iht. § 5-7 besluttet at koblingsstasjonen er gitt klasse 2.

5.2.8 Klassifisering etter ytelse er fastsatt på grunnlag av merkeytelser.

For å ha et enkelt og kontrollerbart mål, er klassifiseringskriteriene fastsatt på grunnlag av samlet merkeytelse på de installerte generatorene, transformatorene, kjelene og varmevekslerne. Ytelser som er angitt i konsesjonen, eller ytelser ved f.eks. midlertidig drift på lavere spenningsnivå, er uten betydning. Unntak fra dette prinsippet kan gjøres dersom det foreligger en saklig begrunnelse.

Samlet generatorytelse utgjøres av merkeytelsen for kraftstasjonen. Dette gjelder for alle generatorene som funksjonelt må regnes å tilhøre én stasjon. Helt fysisk separate anlegg skal normalt regnes hver for seg. Det samme gjelder ved f.eks. bygging av en helt ny stasjon i fjell der den eldre ligger i dagen.

Samlet hovedtransformatorytelse, dvs. transformeringen mellom spenningsnivåer i nettet, utgjør merkeytelsen for transformatorstasjoner. For transformatorer med flere funksjoner (viklinger) regnes høyeste ytelse av transformering mellom nettnivåer. Generatortransformatorer regnes som en del av kraftstasjonen og regnes normalt ikke med i ytelse for transformatorstasjoner. Hvis stasjonen har generatortransformatorer, som også transformerer mellom ulike spenningsnivåer i nettet eller som leverer direkte til lokal forsyning, medregnes den ytelsen som forsyner til nettet i ytelsen til transformatorstasjonen. På linje med rene generatortransformatorer, inngår ikke transformering for reguleringstekniske formål, måletransformatorer, mobile reserve-/beredskapstransformatorer eller midlertidig oppsatte transformatorer i beregning av ytelsen.

Treviklingstransformatorer i kraftstasjoner har som regel lavspenning for generatoren og høyspenning for tilkobling til nettet. Tertiærviklingen kan være for stabilisering eller for å håndtere

enpolet jordslutning, og har sjelden uttak av kraft. Tertiærviklingens ytelse regnes ikke med. Hvis tertiærviklingen har uttak og leverer til forbruksformål, regnes den med i ytelse til nettransformering. I nettanlegg transformerer tertiærviklingen ofte til fasekompensering eller den er uten uttak for å håndtere enpolet jordslutning. I slike tilfeller regnes den ikke med. Av og til har transformatoren tre viklinger for tre forskjellige spenningsnivåer i nettet, og alle tre viklinger regnes med. Samlet transformatorytelse er angitt på merkeskiltet.

Tabell 5: Ytelser til grunn for klassifisering av treviklingstransformator med ulike formål for tertiærviklingen

<i>Transformatorytelse</i>	<i>Primærvikling</i>	<i>Sekundærvikling</i>	<i>Tertiærvikling</i>	<i>Ytelse for klassifisering</i>
100 MVA	100 MVA	80 MVA nett	20 MVA regulering	80 MVA
100 MVA	100 MVA	80 MVA nett	20 MVA nett	100 MVA

5.2.9 Klassifisering etter spenningsnivå (kV) i kraftledninger

Spenningsnivået i kraftledningsanlegg angis i runde tall og skal i praksis forstås som den maksimale spenningen som anlegget er konstruert og isolert for (merkespenning).



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 2-3 Risikovurdering](#)
- [§ 5-3 Sikring av klassifiserte anlegg](#)
- [§ 5-7 Vedtak om sikring eller klasse](#)
- [§ 7-1 Generell plikt til å beskytte driftskontrollsystemet](#)
- [§ 8-9 Forholdet til eldre vedtak om klassifisering og overgangsmatter](#)

Koplinger til annet regelverk

- [Kontrollforskriften](#)
- [Damsikkerhetsforskriften](#)

5.3 Sikring av klassifiserte anlegg



§ 5-3. Sikring av klassifiserte anlegg

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



Denne bestemmelsen er en viktig forutsetning som må legges til grunn ved all vurdering av sikring av anlegg. Kravet er at risikoen blir minst mulig.

De etterfølgende bestemmelsene §§ 5-4, 5-5 og 5-6 stiller tilleggskrav til sikringstiltak av anlegg i klasse 1, 2 og 3. Forskriften stiller ellers krav til å vurdere risiko ved ekstraordinære forhold (se § 2-3) og til risikovurdering i forbindelse med bygging, vesentlig endring eller utvidelse (se § 5-8). Intensjonen med risikovurdering er å avdekke sårbarhet og så sikre anleggene slik at konsekvensen blir minst mulig. Klassifiserte anlegg har viktige samfunnsfunksjoner. Hvis man bare tar bedriftsøkonomiske hensyn og følger minimumskravene uten nærmere vurderinger, er ikke kravet i denne bestemmelsen oppfylt

Sikringsnivå og sikringstiltak skal inngå i anleggets utforming og utførelse. Dette gjelder helt fra stedsvalg foretas og prosjekteringen starter, konsesjonssøknad sendes, melding om sikring sendes og fram til anlegget er i drift med oppfølgende kontroll og vedlikehold. Se mer om meldeplikt om sikringstiltak i § 5-9.



Krav til sikring og andre beredskapshensyn blir langt på vei en del av konsesjonsprosessen. Se gjeldende utgave av NVEs *Veileder for utforming av søknader om konsesjon for nettanlegg*.

Anleggets konstruksjon, tilstand og skirning etter denne bestemmelsen og etter § 5-4 med vedlegg 1, § 5-5 med vedlegg 2 og § 5-6 med vedlegg 3 skal kunne dokumenteres, se også § 2-10 om internkontrollsystem.



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 2-3 Risikovurdering](#)
- [§ 2-10 Internkontrollsystem](#)
- [§ 5-4 Sikringstiltak for klasse 1](#)
- [§ 5-5 Sikringstiltak for klasse 2](#)
- [§ 5-6 Sikringstiltak for klasse 3](#)
- [§ 5-8 Vurdering](#)
- [§ 5-9 Meldeplikt om sikringstiltak](#)

5.4, 5.5 og 5.6 Sikringstiltak for klasse 1, 2 og 3

§

§ 5-4. Sikringstiltak for klasse 1

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

1. Anlegget skal utføres etter krav til normalt sikringsnivå, som nærmere angitt i vedlegg 1
2. Skader og funksjonstap skal oppdages innen rimelig tid
3. Skader skal utbedres og anleggets funksjoner skal gjenopprettes uten ugrunnet opphold

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

§ 5-5. Sikringstiltak for klasse 2

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

1. Anlegget skal utføres og utstyres etter middels høye krav til sikring, som nærmere angitt i vedlegg 2
2. Tap av vitale funksjoner skal begrenses og etter eventuell skade skal anleggets funksjonalitet gjenopprettes uten ugrunnet opphold

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

§ 5-6. Sikringstiltak for klasse 3

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

1. Anlegget skal utføres og utstyres etter høye krav til sikring, som nærmere angitt i vedlegg 3
2. Vitale funksjoner skal opprettholdes i ekstraordinære situasjoner og anleggets funksjonalitet skal gjenopprettes uten ugrunnet opphold

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

5.4-, 5.5- og 5.6 -1 Sikringstiltakenes formål

Bestemmelsene viser til særskilte kravene i hhv. vedlegg 1, 2 og 3. I tillegg viser bestemmelsene til vedlegg 4. Alle kravene i vedleggene er derfor å oppfatte som forskriftsbestemmelser på lik linje med kravene i dette hovedkapitlet.

Sikringstiltakene skal samlet sett forebygge og begrense skader, inntrengning og funksjonssvikt i anlegg og system. De skal bidra til at forsyningssikkerheten så langt som mulig opprettholdes også i ekstraordinære situasjoner.

Kravene til sikringstiltakene etter disse bestemmelsene og de utførte tiltakene skal:

- Forebygge og forhindre uønskede hendelser og handlinger
- Øke evnen til å håndtere ekstraordinære situasjoner som oppstår
- Begrense skadevirkninger og gjenopprette funksjon dersom skade likevel oppstår

Kravene til sikringstiltak er avhengige av anleggenes klassifisering etter § 5-2, og kravene øker med klasse. Sikringstiltakene for klasse 1, 2 og 3 skal utføres etter krav til hhv. normalt, middels høye og høye krav til sikring, se også «8.2 Sammenhengen mellom sikringsnivå i kbf og sikringsklasser i utvalgte europeiske standarder» i vedleggsdokumentet til kapittel 5.



Sjekkliste: Ta hensyn følgende uønskede hendelser

Tap av vitale funksjoner som for eksempel brann, havarier og teknisk svikt.

Naturskade som skred (snø, fjell/stein, jord, kvikkleire,) og flom/oversvømmelse.

Uvær som vind, nedbør (regn/snø), ising og atmosfæriske forstyrrelser.

Inntrengning av uønskede personer og kjøretøy, urettmessig overtakelse og ytre skadeverk (inkludert håndvåpen, splinter og elektronisk påvirkning som jamming og EMP)

5.4-, 5.5- og 5.6- .2 Funksjonsbaserte krav til sikringstiltak

De funksjonsbaserte kravene til sikringstiltak består av fire kategorier:

- a. Oppdagelse og effektiv håndtering av hendelser
- b. Fysisk og elektrisk utførelse og beskyttelse
- c. Rask gjenopprettingsevne
- d. Redundans i anlegg eller system

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

Sikringstiltakene skal, avhengig av anleggets klasse, type, konstruksjon og risikovurdering av anlegget og omgivelsene, samlet representere en balansert kombinasjon av tiltak innenfor de ulike kategoriene. Der det er nødvendig med sikring ut over minimumskravene, se også veiledningen til § 5-3, kan virksomheten selv kombinere de ulike kategoriene. For eksempel kan mangler i redundans i noen tilfeller kompenseres ved god fysisk sikring eller god gjenopprettingsevne. Denne bestemmelsen gir dermed mulighet for ulike tilpasninger og kombinasjoner av løsninger.

5.4-, 5.5- og 5.6- .3 Særskilte krav i vedlegg 1, 2 og 3 for sikring av klassifisert anlegg

I forskriftens vedlegg 1, 2 og 3 er det gitt særskilte krav til sikringstiltak for henholdsvis klasse 1, 2 og 3. Disse tre vedleggene er bygget opp slik at de kan leses uavhengig av hverandre.

Anlegg der det er gitt krav til sikringstiltak, er nærmere beskrevet i veiledningen til § 5-2, og omfatter:

- Transformatorstasjon
- Kraftstasjon
- Selvstendig koblingsstasjon
- Driftskontrollsystem
- Omformerstasjon (er ikke oppført som egen anleggstype, men følger kravene til transformatorstasjon så langt det passer)
- Sambandsanlegg
- Kraftledning (luftledninger og kabler)
- Fjernvarmeanlegg

Vedleggene omhandler sikringskrav innenfor følgende tema:

- Fysisk utførelse og beskyttelse
- Oppdagelse av uønskede hendelser og handlinger
- Effektiv gjenoppretting og reparasjonsberedskap
- Redundans i anlegg og system
- Anleggets egen strømforsyning og nødstrøm
- Kompetent bemanning av anlegg
- Alternativ drift og beredskapsrom
- Kraftledning
- Fjernvarme
- Øvrige tiltak

5.4-, 5.5- og 5.6- 4 Relevante normer og standarder

Se «8 VEDLEGG 4 NORMER OG STANDARDER» i vedleggsdokumentet til kapittel 5.



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 5-2 Klasser](#)
- [§ 5-3 Sikring av klassifiserte anlegg](#)
- [Vedlegg 1 til § 5-4: Særlige krav til sikring for anlegg klassifisert i klasse 1](#)
- [Vedlegg 2 til § 5-5: Særlige krav til sikring for anlegg klassifisert i klasse 2](#)
- [Vedlegg 3 til § 5-6: Særlige krav til sikring for anlegg klassifisert i klasse 3](#)

5.7 Vedtak om sikring eller klasse

§

§ 5-7. Vedtak om sikring eller klasse

Beredskapsmyndigheten kan treffe vedtak om andre eller ytterligere sikringstiltak i medhold av energiloven § 9-2 annet, jf. tredje ledd. Ved vedtak skal det tas hensyn til anleggets eller systemets betydning for kraftforsyningen.

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

NVE er beredskapsmyndighet, og denne bestemmelsen gir NVE myndighet til å treffe de vedtak som angis i bestemmelsen.

5.8 Vurdering

§

§ 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.

5.8.1 Vurdering av risiko ved bygging, endring eller utvidelse av anlegg

Virksomheten skal foreta samlet risikovurdering ved planlegging av sikringstiltak for anlegg. I tillegg skal virksomheten vurdere særskilte lokale forhold, omgivelser og anleggets type for å få et riktig, fullstendig og balansert hele. Konsekvenser av naturgitt skade som endrede klimapåkjenninger, teknisk svikt, tilsiktede ødeleggelser, osv. skal også være inkludert i vurderingene.



Virksomheten må i risikovurderingen legge kravene i §§ 5-3 til 5-6, inkludert vedleggene 1 til 4 til grunn og gjennomføre følgende sikringstiltak:

- ☐ Grunnsikring – med tilpasning til lokale forhold
- ☐ Permanent tilleggssikring
- ☐ Forberedt tilleggssikring

Alle vurderinger og iverksatte tiltak skal dokumenteres i henhold til § 2-10. Internkontrollsystem.

Virksomheten kan ikke velge løsninger som er svakere enn det grunnsikringsnivået som følger av kravene i denne forskriften. Som det framgår av innledningen til kravene i vedleggene 1, 2 og 3, kan andre løsninger aksepteres dersom eieren av anlegget dokumenterer at man oppnår et minst like godt sikringsnivå. Risikovurderingen vil være en del av en slik dokumentasjon.

Risikovurderingen skal først og fremst vurdere sårbarhet og uønskede konsekvenser og fokusere på sikker drift, mulig skade på anlegget og gjenoppretting etter at en skade har skjedd. Dette gjelder også driftskontrollsystemer og sambandsanlegg. Virksomheten skal analysere alle uønskede hendelser som kan tenkes å forkomme innenfor ovennevnte kategorier, selv om sannsynligheten kan virke liten, se også § 2-3.

I vurderingen av risiko for bevisste handlinger som inntrengning og skadeverk, skal virksomheten ta hensyn til bruk av hjelpemidler med lett (for eksempel vanlig håndverktøy) og middels (tyngre verktøy, kjøretøy) tilgjengelighet. For anlegg i klasse 3 skal analysen også dekke mulig bruk av hjelpemidler som i utgangspunktet er lite tilgjengelige. Virksomheten kan i sine vurderinger legge til grunn trusselnivåene A til D som er beskrevet i sikringshåndboka fra Forsvarsbygg.

Resultatet av og erfaring fra den samlede risikovurderingen skal ligge til grunn for planlegging, prosjektering, utføring og sikring av anlegg.



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 2-3 Risikovurdering](#)
- [§ 5-4 Sikringstiltak for klasse 1](#)
- [Vedlegg 1 til § 5-4: Særlige krav til sikring for anlegg klassifisert i klasse 1](#)
- [§ 5-5 Sikringstiltak for klasse 2](#)
- [Vedlegg 2 til § 5-5: Særlige krav til sikring for anlegg klassifisert i klasse 2](#)
- [§ 5-6 Sikringstiltak for klasse 3](#)
- [Vedlegg 3 til § 5-6: Særlige krav til sikring for anlegg klassifisert i klasse 3](#)
- [§ 2-10 Internkontrollsystem](#)

Håndbok

[Sikringshåndboka](#) (Forsvarsbygg)

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.

Hensikten med meldeplikten

Melding om sikringstiltak er en dokumentasjon på at anlegget blir riktig klassifisert og en erklæring om at anlegget blir sikret godt nok i henhold til sin klasse. Sikringstiltak må planlegges og prosjekteres tidlig i prosessen, slik at sikringstiltakene kan utføres på en hensiktsmessig måte uten unødvendige kostnader. NVE bruker også meldingen for å holde oppdatert oversikt over klassifiserte anlegg.



Melding om sikring av konsesjonspliktige anlegg finnes på [nve.no](#).

Husk at meldingsskjemaet inneholder kraftsensitiv informasjon som skal beskyttes, se § 6-2.

Alle anlegg som skal klassifiseres etter § 5-2, er meldepliktige. Det er ikke meldeplikt for nettstasjoner fordi installert ytelse er så lav at stasjonen ikke klassifiseres. Legg merke til at det er meldeplikt for driftskontrollsystemer i klasse 1 (systemer som styrer eller overvåker anlegg i klasse 1). Det er meldeplikt for driftskontrollsystemer som styrer eller overvåker kraftledninger bygget innenfor områdekonsesjonen. Virksomheten skal benytte skjema 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. Virksomheten må også sende oppdatert melding ved endring eller utvidelse av et anlegg eller system.

Meldingen skal 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 «god tid» og ta hensyn til 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, men som et minimum bør virksomheten sende den minst tre til seks måneder for oppstart av arbeidet.



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 5-2 Klasser](#)
- [§ 6-2 Kraftsensitiv informasjon](#)

5.10 Vakthold

§

§ 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.

Plikten omfatter blant annet:

- Påvise anleggets vitale deler og beskaffenhet for øvrig*
- Anskaffe materiell for sikring av anlegget og gjennomføre øvrige tiltak for å hjelpe vaktstyrken*
- Tilrettelegge for øvelser på anleggets område*

Virksomheter som eier anlegg som er prioritert for vakthold, har fått beskjed om dette..

Behov for ekstra vakthold ved utvalgte kraftforsyningsanlegg

Noen kraftforsyningsanlegg er av NVE og andre myndigheter vurdert som særlig viktige eller utsatte. I ekstraordinære situasjoner kan det bli nødvendig å planlegge og etablere ekstra vakthold eller innsats fra

væpnede styrker fra politiet og/eller Forsvaret. Virksomheter med anlegg der dette gjelder blir informert av NVE.

Planlegging og gjennomføring av vakthold

Denne bestemmelsen pålegger en del plikter for eier eller driver av kraftforsyningsanlegg/ objekt som er prioritert for vakthold, herunder å påvise anleggets vitale deler og beskaffenhet til de styrker (politi og forsvar) som skal planlegge vaktholdet.

Ved slik vurdering skal virksomheten legge følgende faktorer til grunn:

- umiddelbare konsekvenser av skade/ødeleggelse
- de ulike anleggenes sårbarhet og beskyttelse
- reparasjonsmuligheter og erstatningstider
- alternativer, muligheter for omlegginger og improvisasjoner

Tilrettelegge for øvelser ved høyspenningsanlegg

Virksomheter skal tilrettelegge for øvelser m.m. ved høyspenningsanlegg. NVE har i samarbeid med DSB fastsatt egne bestemmelser for øvelser i: *Sikkerhetsbestemmelser for øvelser m.m. ved kraftforsyningsanlegg* Dette gir de ulike parter ved slike øvelser klare plikter og rettigheter, og legges til grunn ved alle øvelser i forbindelse med høyspenningsanlegg. Se også veiledning til § 2-7.

Adgang for politi og Forsvar

Energiloven gir etter § 9-5 *Meldeplikt, rett til adgang og vilkår for tilgang* adgang til grunn, bygg og anlegg for politiet og militære myndigheter når dette har sammenheng med forberedelse til og gjennomføring av væpnet sikring. Se også § 9. i *forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg* om adgang.



Krysskopling til andre paragrafer i denne forskriften

- [§ 2-7 Øvelser](#)

Koplinger til annet regelverk

- [Energiloven](#)
- [Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg](#)

Andre veiledere

- Sikkerhetsbestemmelser for øvelser m.m. ved kraftforsyningsanlegg
<https://www.dsb.no/lover/brannvern-brannvesen-nodnett/veiledning-til-forskrift/temaveiledning-om-brannvern-i-kraftforsyningen/#opplaring-og-ovelses>
(lenke til veiledning på DSB, oppdatert veiledning kommer på NVEs nettsider)

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.

Hensikten med bestemmelsen er å **forebygge** kartlegging, lekkasje og spredning av sensitiv og taushetsbelagt informasjon, planlegging og gjennomføring av skadeverk, rettsstridig overtakelse, og bruk av trusler og vold mot personell på anlegg og driftssentraler.

Restriksjoner for adgang til steder og områder gjelder **i tillegg** til sikring av anlegg mot adgang for uvedkommende, jf. § 5-1.

For rubrisert fremstilling av de generelle restriksjonene, se Tabell 6.

Tabell 6: Generelle restriksjoner for gjester og personell i tjenesteoppdrag.

	Gjester	Personell i tjenesteoppdrag
Klasse 1 og 2 – driftssentraler	Fast avgrenset rute (annet ledd bokstav a). Ledsagelse (annet ledd bokstav b). Fotoforbud, med mulig unntak (annet ledd bokstav c).	Fotoforbud, med mulig unntak (annet ledd bokstav c).
Klasse 1 og 2 – anlegg (inkl. lokalkontrollanlegg)	Fast avgrenset rute (annet ledd bokstav a)). Ledsagelse (annet ledd bokstav b) Fotoforbud, med mulig unntak (annet ledd bokstav c).	Fotoforbud, med mulig unntak (annet ledd bokstav c).
Klasse 3 – driftssentraler	Besøksforbud (tredje ledd). Fotoforbud (tredje ledd).	Fotoforbud (tredje ledd). Fysisk adgang krever full bakgrunnssjekk (tredje ledd).
Klasse 3 – anlegg (inkl lokalkontrollanlegg)	Fast avgrenset rute (annet ledd bokstav a). Ledsagelse (annet ledd bokstav b). Fotoforbud, med mulig unntak (annet ledd bokstav c).	Fotoforbud, med mulig unntak (annet ledd bokstav c).

For definisjon av **driftssentral**, se veiledning til § 7-1.

Med **besøkende** menes gjester hvis besøk ikke er knyttet til et konkret tjenstlig behov for anleggets (eller driftssentralens) eier eller driver. Gjester kan være foreninger, skoleklasser, turister, journalister, offentlige virksomheter – når de ikke driver myndighetsutøvelse, eller private selskaper – utenom anskaffelser og leverandørforpliktelser. Listen er ikke nødvendigvis utfyllende.

Personell i tjenesteoppdrag, det vil si personell som er satt til å utføre stedlige oppgaver på vegne av anleggets (eller driftssentralens) eier eller driver, skal ikke regnes som besøkende. Viktigste restriksjon som kommer til anvendelse er fotoforbud

Kravet om full bakgrunnssjekk for adgang til driftssentraler i klasse 3, se tredje ledd, gjelder ved **fysisk adgang**. Bestemmelsene skiller ikke mellom norske og utenlandske statsborgere.

Bestemmelsen gjelder for anlegg som er **i drift** eller **under sikkerhetsmessig ferdigstillelse**. For anlegg som er under delvis drift på grunn av utvidelse, oppgradering eller vedlikehold, må virksomheten vurdere risiko og iverksette egnede tiltak. Et prinsipp er å dele av anlegget i ulike soner med hensyn til personellsikkerhet.



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 5-1 Sikringsplikt](#)
- [§ 7-1 Generell plikt til å beskytte driftskontrllsystemet](#)

5.12 Forholdet til annet regelverk og standarder

Virksomheten er selv ansvarlig for å holde seg orientert om eventuelle endringer i andre regelverk og standarder som er av betydning for det totale sikringsnivået.

Kraftberedskapsforskriftens grunnkrav stiller som regelsom regel strengere krav til sikringstiltak enn andre lover og forskrifter. I andre tilfeller tar ikke kraftberedskapsforskriftens krav alltid hensyn til konstruksjonsmessige og liknede krav i annet regelverk. NVE forutsetter derfor at bygnings-, brann- og elektrotekniske krav til både bygninger, øvrige konstruksjoner og elektriske komponenter beregnes og utføres etter alle gjeldende regler og normer. Dette kan resultere i økte, men ikke reduserte, krav til konstruksjon og utførelse.

Innhold

6. Informasjonssikkerhet	1
6.1 Identifisering av kraftsensitiv informasjon og rettmessige brukere	2
6.2 Kraftsensitiv informasjon	5
6.3 Beskyttelse, avskjerming og tilgangskontroll.....	17
6.4 Sikkerhetsinstruks	21
6.5 Anskaffelser	23
6.6 Begrenset anbudsinnbydelse	25
6.7. Personkontroll	28
6.8 Sikkerhetskopier.....	32
6.9 Digitale informasjonssystemer	34
6.10 Beskyttelse av brytefunksjonalitet i AMS.....	44

6. Informasjonssikkerhet

Kapittel 6 omhandler informasjonssikkerhet. Informasjonssikkerhet har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke. Det handler om å sikre tilgjengelighet til informasjon, integriteten til informasjon (at ingen kan urettmessig endre innhold) og konfidensialiteten til informasjon (kun de med rettigheter kan få tilgang til informasjon).

Informasjon og data er viktige innsatsfaktorer i produksjon, distribusjon og omsetning av elektrisitet og varme. Virksomhetene må beskytte virksomheten sin informasjon og data mot utilsiktet informasjonslekkasje, uautorisert endring og skadeverk, og sikre tilgjengelighet til informasjon og data for brukere med tjenstlig behov. Hvordan virksomheten har oppfylt kravene skal dokumenteres i internkontrollsystemet, se § 2-10.



Taushetsplikt for kraftsensitiv informasjon gjelder for enhver. *Enhver* betyr *alle* som får tilgang eller kjennskap til kraftsensitiv informasjon, både fysiske og juridiske personer.

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.

Virksomheten plikter å identifisere hva som er kraftsensitiv informasjon:

- KBO-enheter har *en plikt* til å identifisere *hva* som er kraftsensitiv informasjon. Det er virksomheten som er ansvarlig for å vurdere verdien på informasjon og hva som er kraftsensitiv informasjon
- Kravet betyr at KBO-enhetene må ha rutiner og praksis der ansatte som behandler informasjon, gjør en selvstendig vurdering av hvilken informasjon som er å anse som kraftsensitiv, og hva som ikke er kraftsensitivt. Kraftsensitiv informasjon må merkes, se § 6-3

Virksomheten plikter å identifisere hvor kraftsensitiv informasjon befinner seg:

- På samme måte som det er nødvendig å identifisere *hva* slags informasjon man skal beskytte, er det en forutsetning for å kunne iverksette gode tiltak, at man vet *hvor* informasjonen er lagret eller blir behandlet. Hvor betyr for eksempel i eget fysisk arkiv, egen fysisk eller virtuell server eller i ekstern lagrings- og behandlingstjeneste hos avtalepart. Vi viser til § 6-5. Se også [råd fra Direktoratet for økonomiforvaltning om anskaffelser av skytjenester](#). Forum for sikkerhet i kraftforsyningen (FSK) har laget en veiledning for Microsoft 365
- Bestemmelsen er utformet slik at kravet omfatter ulike lagringsmåter for kraftsensitiv informasjon. Formuleringen «*lagring på annen måte*» understreker at oppbevaring på papir og lagring i elektronisk form ikke er en uttømmende liste. Eksempel på annen måte kan være videoopptak eller microfilm. KBO-enhetene skal ha system og rutiner for å håndtere all kraftsensitiv informasjon slik forskriften krever, uavhengig av hvor informasjonen er lagret. Når kraftsensitiv informasjon skal behandles av leverandører eller samarbeidspartnere, må KBO-enheten regulere denne informasjonsbehandlingen i en egen sikkerhetsavtale med leverandøren eller samarbeidspartneren

Virksomheten plikter å identifisere hvem som har tilgang til kraftsensitiv informasjon. Det innebærer at de har oversikt over hvem som har fått tilgang til og oppbevarer kraftsensitiv informasjon som virksomheten er ansvarlig for. Tilgang til kraftsensitiv informasjon bør logges også når ansatte hos leverandør får tilgang. Virksomheten bør derfor stille krav til logging i avtaler med leverandør og kunne gjøre rede for hvem som har hatt tilgang, lest og endret informasjon, i en eventuell revisjon utført av virksomheten selv eller av tredjepart på vegne av virksomheten.

Det er KBO-enhetene som eier sin kraftsensitive informasjon og som har ansvaret for å vurdere hvem som er rettmessige brukere.

KBO-enhetene skal vurdere sikkerheten ved all behandling av kraftsensitiv informasjon. Dette innebærer blant annet å sørge for at ingen andre enn «*rettmessige brukere*» får tilgang eller kjennskap til sensitiv informasjon om kraftforsyningen», se § 6-4.

Med rettmessig bruker menes «*fysiske eller juridiske personer som har tjenstlig behov for kraftsensitiv informasjon.*» Utgangspunktet for vurderingen er hvorvidt KBO-enheten selv har tjenstlig behov for å dele kraftsensitiv informasjon for å kunne utføre sine oppgaver. Det er primært følgende grupper som, etter en konkret vurdering, er rettmessige brukere, jf. [Prop 112 L\(2010-2011\)](#):

- selskapets egne ansatte som trenger tilgang for å utføre pålagt arbeid
- leverandører og andre samarbeidspartnere som KBO-enheten har inngått avtale med
- myndigheter med tilsynsansvar og etater med beredskapsansvar (medlemmer av fylkesberedskapsrådet m.fl.)

Nøyaktig kartfesting av jordkabler er informasjon som det kan være tjenstlig behov for å dele med kommuner og berørte parter etter *plan- og bygningsloven* § 2-3. Det er i KBO-enhetens interesse å unngå graveskader og kabelbrudd.

Dersom det foreligger et tjenstlig behov for å videreformidle kraftsensitiv informasjon, skal deling skje på en måte som gjør at uvedkommende ikke får tilgang til informasjonen. Informasjon kan deles over sikret nett eller i sikret tjeneste, eventuelt på åpen e-post der vedlegg som inneholder kraftsensitiv informasjon er kryptert, se også § 6-3.

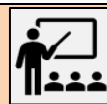
Den som har fått tilgang til kraftsensitiv informasjon fra KBO-enheten, kan ikke dele denne informasjonen videre uten samtykke fra KBO-enheten. Dette følger av fjerde ledd.

Eksempel: Identifisering av kraftsensitiv informasjon



IKT-sikkerhetskoordinator i Kraftkonsernet AS er kjent med at virksomheten må identifisere kraftsensitiv informasjon etter kbf § 6-1. Denne informasjonen ligger i ulike systemer i virksomheten, på servere, i klienter og i fysisk arkiv, i databaser, i styringssystemer, i vedlikeholdssystemet, i administrative systemer.

Ved en stikkprøve viser det seg at ikke all kraftsensitiv informasjon er merket. IKT-sikkerhetskoordinatoren anbefaler for ledelsen at de kjører en intern kampanje på hva som er kraftsensitiv informasjon, hvordan den skal merkes, lagres og sikres i overføring mellom ulike tjenester og personer. Mange trenger tilgang til kraftsensitiv informasjon. Det inkluderer også eksterne, inklusive leverandører, og offentlige etater. Merking av informasjon er viktig for å vite hvilken informasjon som er underlagt taushetsplikt og som skal beskyttes.



Eksempel: Rettmessig bruker og sikring av kraftsensitiv informasjon

Nett AS får en forespørsel fra en forskningsinstitusjon om å bli med i et forskningsprosjekt på digitalisering av lokalkontrollanlegg. Dette innebærer at forskerne må få tilgang til kraftsensitiv informasjon. Ledergruppen anbefaler at Nett AS blir med i forskningsprosjektet fordi det har relevans og nytteverdi for virksomheten. IKT-sikkerhetskoordinator vurderer derfor at forskerne er rettmessige brukere av kraftsensitiv informasjon.

Nett AS inngår sikkerhetsavtale med forskningsinstitusjonen og bruker NVEs mal for sikkerhetsavtale. Her er det regulert hvordan kraftsensitiv informasjon skal behandles og beskyttes. En av forskerne i prosjektet er Nett AS sin egen nyansatte PhD-student. Han må signere taushetserklæring. Nett AS benytter NVEs mal for taushetserklæring.

Leverandører og andre som har fått tilgang til kraftsensitiv informasjon fra KBO-enheten, kan ikke dele denne videre uten samtykke fra KBO-enheten. Dette er fordi det er KBO-enheten som avgjør hvem som er rettmessige brukere. Dette forholdet må etter § 6-5 reguleres i en sikkerhetsavtale som skal inngås mellom KBO-enheten og leverandøren.



Eksempel: Videreformidling av kraftsensitiv informasjon

Nett AS er med i et forskningsprosjekt og har inngått avtale med et forskningsinstitutt. Forskningsinstituttet mister viktig kompetanse da en ansatt slutter, og det oppstår et behov for at forskningsinstituttet engasjerer en ekstern konsulent for å bistå i arbeidet videre. Forskningsinstituttet kan ikke overføre kraftsensitiv informasjon til konsulenten uten Nett AS sin godkjenning. Den eksterne konsulenten må også inngå en avtale om behandling av kraftsensitiv informasjon med Nett AS. Konsulentselskapet har sin egen standardavtale. Denne kan brukes når den gir tilsvarende beskyttelse av kraftsensitiv informasjon som NVEs mal for sikkerhetsavtale.

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, system eller annet 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 samfunnsviktige 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*

Bestemmelsen krever skjønnsmessig vurdering av informasjonseier eller behandler. Bestemmelsen

- inneholder en *generell definisjon* av hva som er å anse som kraftsensitiv informasjon
- inneholder en *ikke-uttømmende liste med konkrete eksempler* på typer informasjon som er kraftsensitiv i bokstav a-j
- innebærer også at annen informasjon enn den som er opplistet i bokstav a-j kan være kraftsensitiv. Det vil da måtte avgjøres etter den generelle definisjonen i annet ledd første setning
- innebærer også at sammenstilling av ulik informasjon som ellers ikke omfattes av bestemmelsen til sammen kan gi så spesifikk og inngående kjennskap at den må anses som kraftsensitiv etter den generelle definisjonen

Taushetsplikt for kraftsensitiv informasjon

Bestemmelsen viser til taushetsplikten for kraftsensitiv informasjon etter *energiloven* § 9-3. Denne taushetsplikten gjelder for enhver og lyder:



Energiloven § 9-3 (Informasjonssikkerhet) annet ledd

«Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen.»

Enhver betyr alle som får tilgang eller kjennskap til kraftsensitiv informasjon, både fysiske og juridiske personer. At informasjonen er underlagt taushetsplikt, betyr at man skal sørge for at ikke andre enn rettmessige brukere får tilgang til kraftsensitiv informasjon. Dette innebærer blant annet at informasjonen ikke skal være søkbar på internett, tilgjengelig for ikke autoriserte brukere eller publisert offentlig.

Hva omfattes av den generelle definisjonen?

Det er kun informasjon som utgjør «spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen.» som er kraftsensitiv informasjon.

Bestemmelsen angir to kjennetegn, som begge må være til stede, for at informasjon vil være å anse som kraftsensitiv:

- Informasjonen må være *«spesifikk og inngående»*. Med spesifikk menes konkret, for eksempel et konkret anlegg eller system. Med inngående menes detaljert. Dette stiller krav til at opplysningene må være mer enn kun oversiktspreget og ha en viss detaljeringsgrad. Bokstav a-j kommer nærmere inn på eksempler på hva som menes med spesifikke og inngående opplysninger i forskjellige tilfeller. Spesifikk og inngående opplysninger vil for eksempel kunne være en teknisk tegning eller bilde med detaljer av et klassifisert anlegg sammen med geografisk lokalisering eller navn på anlegget
- Informasjonen må videre være av en slik art at den *«kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen.»* Dette innebærer at misbruk av opplysningene til sabotasjeformål har et skadepotensial. Virksomheten trenger ikke å vite med sikkerhet at skade vil oppstå eller at funksjoner faktisk blir påvirket dersom dette skjer, men det er tilstrekkelig at virksomheten anser det som sannsynlig at misbruk av opplysningene kan få slike følger. Når konstruktive detaljer og tilgjengeligheten til anlegget er synliggjort, er det både spesifikk og inngående informasjon. Også sammenstilling av opplysninger, som alene ikke anses som sensitive, kan gi så spesifikk eller inngående informasjon om kraftforsyningen eller anlegg at den kan brukes til å skade anlegg, system eller annet, eller påvirke funksjoner på en måte som har betydning for kraftforsyningen



Eksempel: Informasjon som ikke er kraftsensitiv

- Opplysninger av generell og oversiktspreget art om kraftforsyningen
- Kart over luftledninger med spenningsnivå
- Bilder av anlegg som kraftledninger, bygninger og infrastruktur som er synlige for allmennheten i terrenget. Merk at detaljinformasjon om de samme anleggene, eks. lås- og alarmsystem på bygg, er kraftsensitiv informasjon

Hva omfattes av listen i bokstav a – j?

Bokstav a-j gir eksempler, og disse eksemplene er ikke-uttømmende. KBO-enheten må i tillegg foreta en selvstendig og skjønnsmessig vurdering av om de har informasjon utover oppstillingen som kan være sensitiv etter den generelle definisjonen.

Bokstav a

«Alle systemer som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband»

Systemer som ivaretar driftskontrollfunksjoner betraktes som kraftsensitiv når informasjonen om disse systemene også er spesifikke og inngående. Det ville innebære for eksempel opplysninger om leverandør, produktnavn, produktnummer, versjonsnummer, funksjonalitet og geografisk lokalisering.



Eksempel: Kraftsensitiv informasjon og besøk på driftssentral

IKT-sikkerhetskoordinator i Nett AS har fått en forespørsel fra sin leverandør av driftskontrollsystem om leverandøren kan ta med noen utenlandske kunder hos denne leverandøren på besøk. Nett AS har nylig bygget ny driftssentral med et moderne driftskontrollsystem, klasse 3. IKT-sikkerhetskoordinatoren vurderer at «systemer som ivaretar viktige driftskontrollfunksjoner», altså driftskontrollsystem er vidtrekkende. Det dekker eksempelvis koplingsbilder, skiftordning for personell, selve SCADA-systemet med skjermer, kommunikasjonssystem og full oversikt over nettanlegg, annet IT-utstyr på sentralen, fysisk låsesystem og soneinndeling, andre sikringstiltak, samt beredskapsrommet.

Tilgang til kraftsensitiv informasjon krever tjenstlig behov. Det er ikke tilfelle her. Besøket skal informere leverandørens kunder. Besøk på driftssentralen er også regulert i § 5-11. Nett AS kan ta imot besøk på et av møterommene hos virksomheten, men ikke ta med besøkende inn på driftssentralen i klasse 3. I forkant av møtet har Nett AS et internt møte der de forbereder hvilken informasjon som kan deles og hvordan besøkende skal tas imot og følges.

Bokstav b

«Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg»

Med detaljert informasjon om energisystemet menes informasjon om hvordan anlegg for produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi og fjernvarme inngår i et system. Både enlinjeskjema og informasjon om hva det viser formidlet ved tekst, video eller tale, er kraftsensitiv informasjon.

Enlinjeskjema kan inneholde detaljer om anlegg og hvordan anleggene henger sammen i kraftsystemet, og vil derfor være å anse som sensitivt. Det er imidlertid en forutsetning at informasjonen er både «spesifikk og inngående».

Enkle og lite detaljerte oversikter over kraftnettet på et aggregert nivå, vil falle utenfor hva forskriften definerer som kraftsensitiv informasjon. Det at oversikten er aggregert betyr at den *ikke* viser brytere og samleskinner eller annen informasjon som gjør det mulig å utlede sensitive opplysninger om kraftnettets funksjonalitet, som for eksempel koblingsmuligheter og alternative forsyningsveier. I en aggregert oversikt kan en transformator- eller koblingsstasjon presenteres som ett enkelt punkt og en ledning som én enkelt linje uten at dette er kraftsensitivt.

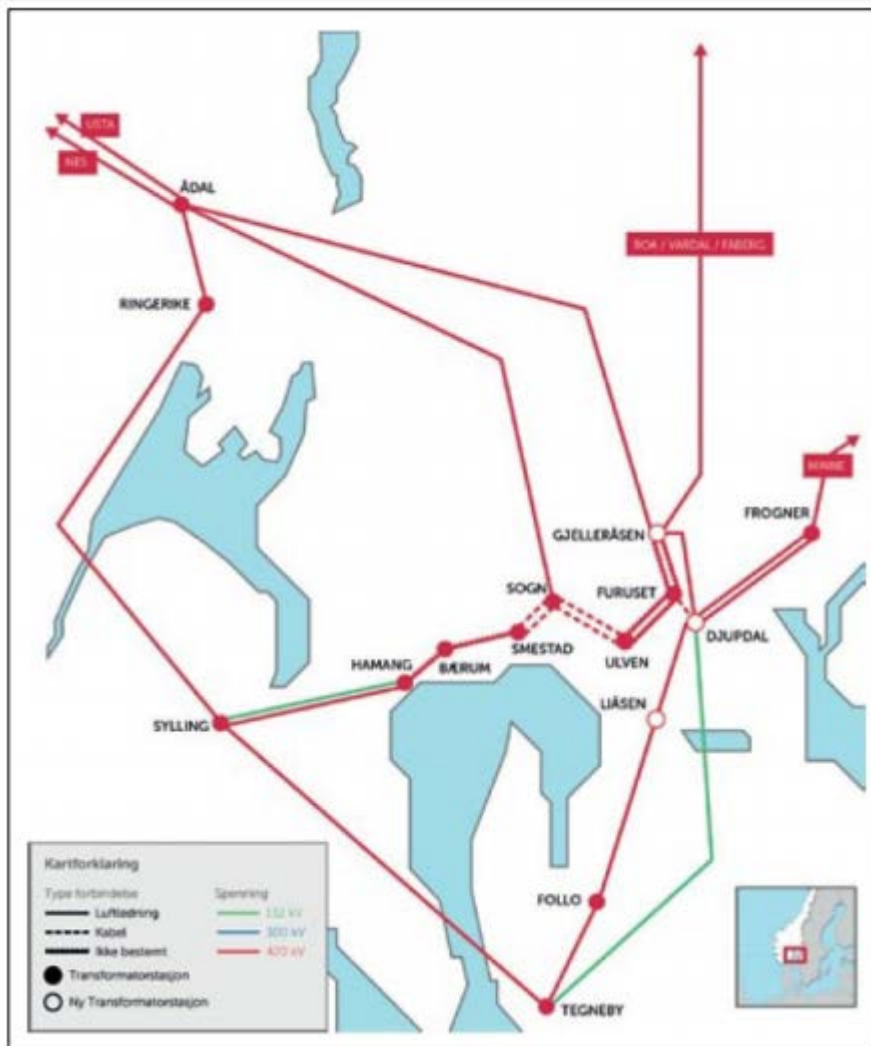
Dronefilmer over anlegg med geotagging kan derfor fort inneholde kraftsensitiv informasjon etter denne tolkningen.

Eksempel: Oversiktskart som ikke er kraftsensitivt

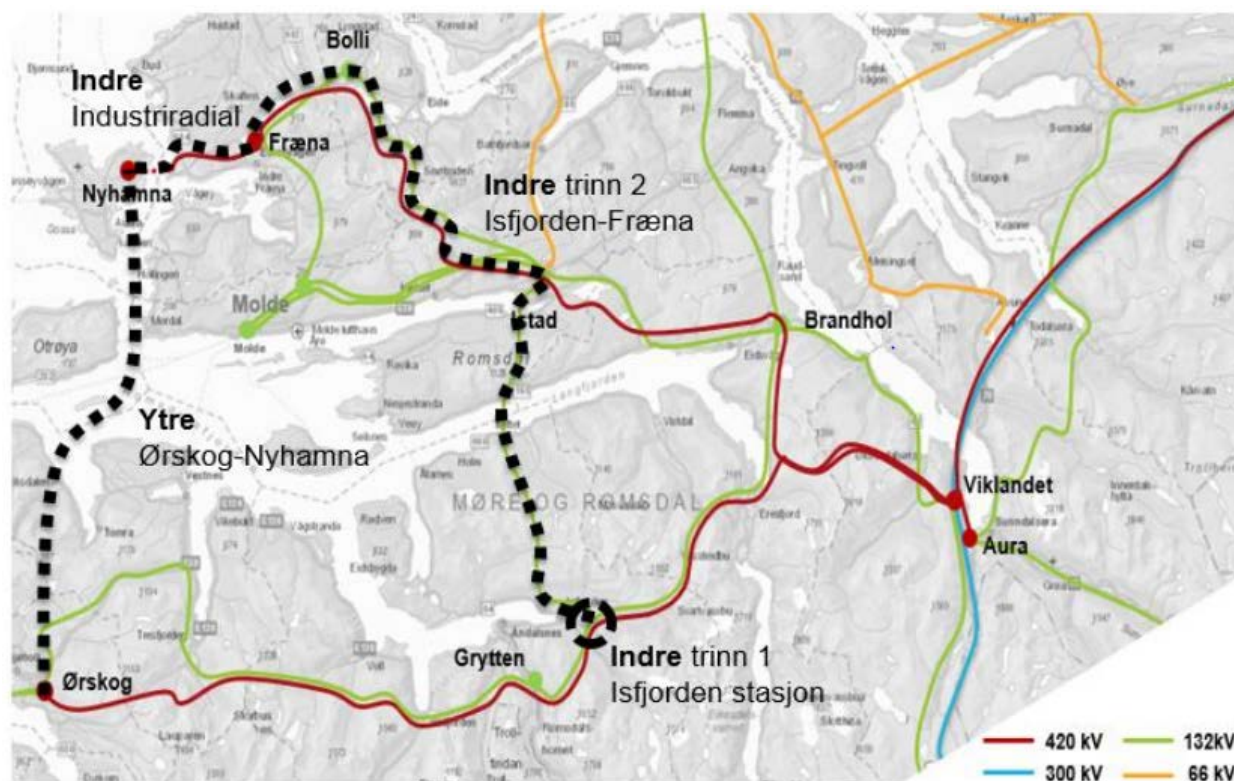


Nett AS planlegger å bygge om kraftsystemet inn til en større by i sitt forsyningsområde. På møte med berørte kommuner viser de en oversikt over nåværende og planlagte ledninger og transformatorstasjoner. Oversikten viser spenningsnivå på ledningene. Denne oversikten inneholder så få detaljer at den kan vises offentlig.

Bildene nedenfor er eksempler på lite detaljerte oversikter over kraftnettet på et aggregert nivå.



Figur 1: Fra Statnetts konseptvalgutredning (KVU) «Nettplan Stor-Oslo» fra 2013 som per i dag er offentlig informasjon. Oversikten viser planlagt overordnet nettstruktur for transmisjonsnettet i Oslo og omegn (<https://www.statnett.no/vare-prosjekter/region-ost/nettplan-stor-oslo/>).



Figur 2: Fra Statnetts KVV «Bedre leveringspålitelighet i kraftforsyningen til Nyhamna» fra 2015 som per i dag er offentlig informasjon. Kartet viser en oversikt over både transmisjons- og regionalnett i Møre og Romsdal. Transformatorstasjoner er representert som ett aggregert punkt (<https://www.statnett.no/globalassets/for-aktorer-i-kraftsystemet/planer-og-analyser/konseptvalgutredning-nyhamna.pdf>).

Forskriften angir at enlinjeskjema for mindre viktige produksjonsanlegg ikke er sensitivt. Mindre viktige produksjonsanlegg er produksjonsanlegg som verken har betydning for samfunnskritisk virksomhet eller forsyningssikkerheten til et stort antall kunder.

Bokstav c

«Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygging og drift»

Detaljert informasjon om klassifiserte transformatorstasjoner er sensitiv informasjon. Med detaljert informasjon om klassifiserte transformatorstasjoner menes anleggets klasse, tekniske egenskaper, informasjon om komponentene i stasjonen, beskrivelse av sikringstiltak og bygningstegninger.

Større transformatorer har lang reparasjonstid og lang leveringstid. Dette innebærer at informasjon som kan benyttes for å identifisere hvilke transformatorer som kan erstatte hverandre i nettet (reserver), er sensitiv informasjon.



Eksempel: Generelle konsesjonssaker

NVE ber om kart/plantegninger over transformatorstasjoner i konsesjonssøknader. Disse legges ut offentlig i forbindelse med høringer, med mindre det er merket som kraftsensitivt. Det er derfor viktig at KBO-enheten merker dokumentene korrekt. Dokumenter med kraftsensitiv informasjon skal merkes **Underlagt taushetsplikt etter energiloven § 9-3 se. kbf. § 6-2. Unntatt fra innsyn etter offentleglova § 13, se eller § 6-2.** Når søkeren har merket dokumentet som angitt, vil NVE skjerme informasjonen.



Eksempel: BIM-modell

Vannkraft AS bygger ny transformatorstasjon. Entreprenøren har designet ny stasjon i BIM – Bygnings Informasjons Modellering. En slik BIM-modell av en transformatorstasjon kan inneholde kraftsensitiv informasjon da den er en digital speiling av en reell stasjon. BIM-modellen kan dermed ikke publiseres. Eksempelet gjelder også digitale tvillinger som blir kopier av kraftanlegg eller systemer.

Bokstav d

«Oversikt over fordelingsnett til samfunnsviktige funksjoner. Oversikt over rørnett for fjernvarme til samfunnsviktige funksjoner»

Formålet med dette kravet er at det ikke skal være enkelt hverken i terrenget, på et offentlig tilgjengelig kart eller på annen måte å se at fordelingsnett og rørnett forsyner en samfunnsviktig funksjon eller hvilken stasjon den kommer fra. Fordelingsnett betyr i denne sammenheng lokalt distribusjonsnett.



Eksempel: Fordelingsnett til sykehus

En utbygger i en kommune ber Nett AS om oversikt over fordelingsnettet til et sykehus lokalisert i nærhet av det planlagte anleggsområdet. Informasjon om fordelingsnettet til sykehus vil være kraftsensitiv informasjon og skal ikke publiseres. Slik informasjon må imidlertid deles med entreprenøren, teknisk etat i kommunen og beskyttes i samsvar med kravene i kraftberedskapsforskriften. Dette reguleres i en sikkerhetsavtale med leverandør og kommune.

Samfunnsviktige funksjoner inkluderer virksomheter med viktig betydning for samfunnets sikkerhet og beredskap. I en kommune kan dette inkludere kommunehuset under beredskap, helsehus, politistasjonen, lokalsykehuset og skolen når den er evakueringsplass. Dette vil også gjelde skjermingsverdige objekter og infrastruktur etter sikkerhetsloven. Det vil kunne variere over tid både hva som er samfunnskritisk virksomhet og hvor denne virksomheten er lokalisert.

Bokstav e

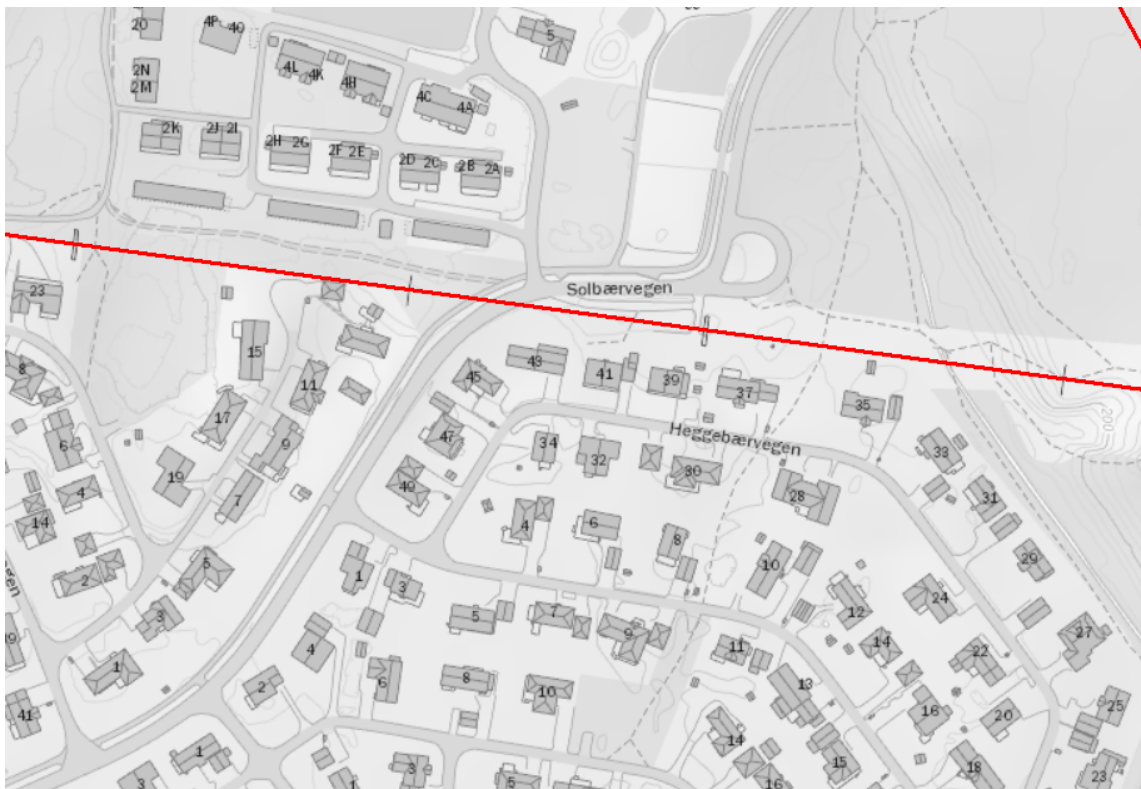
«Nøyaktig kartfesting av jordkabler. Nøyaktig kartfesting av rørnett i fjernvarmeanlegg med varmesentraler i klasse 2»

Nøyaktig kartfesting (spesifikk og inngående informasjon) av jordkabler og rørnett i fjernvarmeanlegg klasse 2 er kraftsensitiv informasjon. Ved å skjerme nøyaktig informasjon om jordkabler, sikrer man at allment tilgjengelig informasjon om luftledninger ikke nødvendigvis viser hele kraftsystemet.

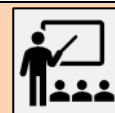
Ved inntegning på offentlig kart kan ikke jordkabler og rørnett i fjernvarmeanlegg med varmesentraler i klasse 2 kartfestes nøyaktig. For at kartfesting *ikke* skal være nøyaktig, må den gjøres på følgende måte:

- Som hovedregel skal kartet ikke ha en større målestokk (mer detaljert) enn 1:2000
- Jordkabler og rørnett skal tegnes inn som én strek ikke smalere enn tilsvarende 3 meter i kartet, ved målestokk 1:2000. Slik unngår man at hver kabel i kabelsettet blir vist. En viss bredde på streken vil gi et visst slingringsmonn hvor kablene/rørene vil bli lagt
- Behov for mer nøyaktig kartfesting må vurderes i det enkelte tilfellet

Karteksempelet nedenfor viser målestokk 1:2000 og en trasébredde på cirka 3 meter.



Figur 3 Eksempel på kartfesting av jordkabler som ikke er kraftsensitiv



Eksempel: Kartfesting av rørnett

Fjernvarme AS er bedt av kommunen om å kartfeste rørnettet i distribusjonsnettet til fjernvarmeanlegget som har varmesentral i klasse 2. Kommunen vil publisere denne informasjonen på kommunens nettside slik at den er lett tilgjengelig for allmenheten. Kartfestingen gjør de ved å tegne inn rørnettet med rett strek mellom to punkter i kartet. Kartet har en målestokk på 1:2000 og streken som er inntegnet er ikke smalere enn 3 meter i terrenget. På denne måten er det ikke detaljert kartfesting og ikke kraftsensitiv informasjon.

Bokstav f

«Forebyggende sikkerhetstiltak mot bevisst skadeverk»

Forebyggende sikkerhetstiltak mot bevisst skadeverk omfatter tiltak i forbindelse med forsterkninger av bygg, IKT-sikkerhetstiltak, vaktordninger, sikringsrutiner, lås, alarm- og overvåkningssystemer m.m. Eksempler er:

- Informasjon om systemer, planer og rutiner for overvåkning, alarm og reaksjon
- Lås- og adgangskontrollsystemer

- Bygningstekniske tiltak som forsterkning av dører, vinduer, transformatorceller og andre konstruksjoner
- Informasjon om IKT-sikkerhetstiltak og sikkerhetsarkitektur
- Rutiner for vaktordninger og planer for bemanning av anlegg
- Rutiner for innleid vekterselskap
- Beredskapsrom – lokalisering i bygget, adgangskontrollsystem og utforming

Bokstav g

«Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift»

Lokalisering av reservedriftssentralen skal ikke være offentlig kjent. Dette gjelder uavhengig av om driftskontrollfunksjoner utøves fra et kontrollrom eller om driftskontrollen kan utøves ved hjelp av hjemmевaktordninger.

Med særskilte beredskapsanlegg menes eksempelvis:

- Mobile sambandscontainere
- Beredskapslager med kritiske komponenter
- Mobile nødstrømsaggregat
- Beredskapsrom og reserveanlegg

Listen er ikke-uttømmende. KBO-enhetene må selv vurdere hva som er særskilte beredskapsanlegg for ledelse og drift.



Eksempel: Reservedriftssentral

En journalist i lokalavisa har publisert en artikkel om den nye driftssentralen og beredskapsrommet til Vannkraft AS. Reportasjen om den nye driftssentralen formidler også at den gamle driftssentralen nå blir en reservedriftssentral. I artikkelen omtales også lokasjonen og fasilitetene til den gamle driftssentralen. Journalisten har fått opplysningene fra Vannkraft AS. Reportasjen inneholder kraftsensitiv informasjon og utgjør et brudd på taushetsplikten i *energiloven* § 9-3 og *kraftberedskapsforskriften* § 6-2.

Vannkraft AS kontakter lokalavisen og ber om at de fjerner artikkelen.

Bokstav h

«Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk»

Virksomhetens risiko- og sårbarhetsvurderinger og andre detaljerte og spesifikke analyser av ekstraordinære og uønskede hendelser og tilhørende beredskapstiltak er kraftsensitiv informasjon.

Generelle begrunnelser i for eksempel konsesjonssaker, som at forsterking av nettet er nødvendig for å redusere generell sårbarhet, er ikke kraftsensitiv informasjon. Dersom man legger til detaljerte

beskrivelser om utfall i tid eller sted koplet til konkrete scenarier, så er dette å anse som kraftsensitiv informasjon. Under dette punktet kommer også detaljerte analyser av kraftsektorens eller kraftsystemets sårbarhet, inkludert digital tvilling som gir spesifikk og inngående informasjon om anlegg eller system eller avslører systemsårbarhet.

Informasjonen som deles, må sikres i henhold til kravene i §§ 6-3 til 6-6.



Eksempel: Presentasjon på åpent brukermøte i regi av interesseorganisasjon

Vannkraft AS presenterer erfaringene etter en kritisk feil i et kontrollanlegg på et åpent brukermøte hos en interesseorganisasjon i bransjen. På brukermøtet er også journalister og leverandører til stede. Feilen er rettet av leverandøren og eksisterer ikke lenger. Vannkraft AS har derfor vurdert at den ikke lenger utgjør en detaljert sårbarhet. Vannkraft AS velger å ikke angi sted/navn på anlegg eller navn på leverandør, men vektlegger å formidle hvordan de oppdaget og håndterte denne hendelsen. Vannkraft AS velger å ikke lage plansjer med inngående og spesifikke opplysninger om dette anlegget. Informasjonsformidlingen her er tillatt og ikke et brudd på forskriftens krav om taushetsplikt.

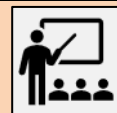
Bokstav i

«Beredskapsplaner for å håndtere bevisst skadeverk»

De planene KBO-enheten har for å håndtere bevisst skadeverk, er kraftsensitiv informasjon. Uvedkommende skal ikke få kjennskap til nøyaktig hvilke konsekvenser ulike typer skadeverk får, og skal heller ikke få kjennskap til beredskapsplaner slik at de kan hindre eller forsinke KBO-enhetens håndtering og evne til rask gjenoppretting

Dersom andre hendelser har samme konsekvens som bevisst skadeverk, er også beredskapsplanene for slike hendelser å regne som kraftsensitiv informasjon. Mange tiltak, prosedyrer og ressurser benyttes uavhengig av hendelsesårsak.

Bokstav h er imidlertid ikke til hinder for at slik kraftsensitiv informasjon kan deles med berørte offentlige etater som kommuner, politi, brannetat, statsforvalter m.fl, eller med KraftCERT, andre KBO-enheter eller leverandører, når det foreligger et tjenstlig behov. Virksomheten kan gi generell informasjon om pågående uønskede hendelser og konsekvenser for kundene.



Eksempel: Beredskapsplan

Kraftkonsernet AS tar i bruk skyteknologi. Beredskapslederen lurte på om beredskapsplan og innsatsplan for ulike hendelser kan legges i skyen. IKT-koordinatoren sender epost til NVE. I svar fra NVE gis det informasjon om at dette er kraftsensitiv informasjon som må beskyttes, og at virksomheten må ha streng tilgangsstyring, godt passordregime og god beskyttelse av informasjonen i form av kryptering av data i ro og i transitt. NVE peker på viktigheten av å ha kontroll på krypteringsnøkklene og minimere risikoen for at utenforstående får tilgang til disse, og ev. supplere med sikkerhetsprosedyrer som hindrer at ansatte hos leverandøren får tilgang til kraftsensitive data uten godkjenning fra Kraftkonsernet AS på forhånd.

I tillegg må Kraftkonsernet AS sikre at virksomheten alltid har tilgang til en lokal kopi av beredskapsplanen, også om skytjenesten ikke skulle fungere eller forbindelsen til serveren skulle bli brutt.

Bokstav j

«Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk»

Denne informasjonen er sensitiv fordi informasjonen samlet sett angir en lagerbeholdning og ressurser knyttet til beredskap for å håndtere bevisst skadeverk. Kravet er relatert til bokstav i. Les mer om reservemateriell og reparasjonsberedskap i kapittel 4.



Eksempel: Database over samlet lagerbeholdning

Leverandør AS drifter en database for flere selskaper i bransjen over samlet lagerbeholdning av reservemateriell. Denne databasen inneholder dermed kraftsensitiv informasjon og må ha streng tilgangsstyring til data og beskyttelse av dataene.

Resten av kapittel 6 oppstiller krav til sikring av kraftsensitiv informasjon (§§ 6-3 - 6-10).



Maler

Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se [NVE maler](#)

NVEs mal for taushetserklæring på norsk og engelsk se [NVE maler](#)

Veiledere

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(norsk\)](#)

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(engelsk\)](#)

[Metode for å finne kraftsensitiv informasjon på internett](#)

[Nettvett Sikker sletting](#)

Krysskopling til annet regelverk

[Lov om nasjonal sikkerhet \(sikkerhetsloven\)](#)

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.

Ordforklaring

<i>Beskyttelse</i>	Verne og forsvare mot misbruk, uønsket tilgang og urettmessig endring
<i>Avskjerming</i>	Forhindre tilgang totalt for andre enn rettmessige (godkjente) brukere
<i>Tilgangskontroll</i>	Mekanisme for å styre adkomst eller tilgang til informasjon, digitale tjenester, IT-systemer, dokumenter og rom. Tilgang styres med utgangspunkt i en sikkerhetsinstruks som virksomhetens ledelse har godkjent
<i>Mobile enheter</i>	Smarttelefoner, nettbrett, kameraer, bærbare pc-er og liknende som kan kobles opp mot et nettverk eller internett
<i>System og rutiner</i>	Med dette menes internkontrollsystem/styringssystem for informasjonssikkerhet, se også § 2-10.

Hvordan oppfylle kravet

Virksomheten må etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Virksomheten må sørge for at tiltakene som nevnt i bestemmelsen er inkludert og dokumentert i internkontrollsystemet:

- Tiltak mot avlytting og manipulering fra uvedkommende
- Merking av dokumenter, oppbevaring, bruk, distribusjon og tilintetgjøring
- Rapportering av hendelser av betydning for informasjonssikkerheten
- Sikkerhetsregler for bruk av mobile enheter

Tiltak som vurderes for tilgangskontroll og beskyttelse bør omfatte:

- Administrative tiltak, herunder sikkerhetsinstruks, taushetserklæringer og sikkerhetsavtaler
- Tekniske tiltak, herunder teknisk sikring av printere, bærbare PC-er, mobile enheter gjennom tilgangsstyring, passordpolitikk som anbefalt av NSM, oppdatering av programvarepolicy, soneinndeling, overvåkning og logging mm, se ellers § 6-9. Ved logging må behandling av personopplysninger være i samsvar med personopplysningsregleverket
- Organisatoriske tiltak for bevisstgjøring og opplæring av ansatte og innleid personell
- Fysisk tiltak for å sikre effektiv tilgangskontroll og beskyttelse, eks. lås på rom

Se mer om tiltak under § 6-5.



Merk at kravene i § 6-3 om beskyttelse, avskjerming og tilgangskontroll også gjelder for analog informasjon og manuelle informasjonssystemer.

Merking av kraftsensitiv informasjon

Bestemmelsen oppstiller en plikt til å merke kraftsensitiv informasjon. Databaser som inneholder kraftsensitiv informasjon, kan merkes gjennom navngivning og koding, eks. **“U-OFF-navn”**. Merk at offentleglova gjelder ikke for private virksomheter (se offentleglova § 2). Private aktører merker kun iht. energiloven og kbf. NVE anbefaler at merking av dokumenter gjøres på denne måten:

Merking av kraftsensitiv informasjon (Bokmål)	Merking av kraftsensitiv informasjon (Nynorsk)
Underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt fra innsyn etter offentleglova § 13.	Underlagd teieplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt frå innsyn etter offentleglova § 13.
Labeling of power sensitive information Subject to duty of confidentiality according to section 9-3 of the Norwegian Energy Act. Exempted from inspection according to section 13 of the Norwegian Freedom of Information Act.	



Eksempel: Nyansatt

En nyansatt i en stilling hos Vindkraft AS må ha tilgang til datanettverk og servere, og virksomhetens kontorlokaler. Nærmeste overordnet til den nyansatte bestiller tilgang til IT-tjenester med utgangspunkt i stillingsbeskrivelsen og ansvarsområdet. IT-drift setter opp hvilken tilgang vedkommende skal ha til IT-tjenester i virksomheten. Den ansatte må gjennomgå opplæring og signere på taushetserklæring og regelverk for bruk av IT-ressurser og mobile enheter. Virksomhetens krav til passordstyrke er konfigurert i systemet og bygger på NSMs passord-råd, og virksomheten administrerer oppretting og sletting av brukere, samt sikring av bærbar PC og ansatt-mobiltelefon.

Tiltak og prosedyrer inngår i virksomhetens internkontrollsystem for informasjonssikkerhet.



Eksempel: Sikker sletting

Nett AS skal skifte ut noen servere og mobiltelefoner. IKT-sikkerhetskoordinator vurderer ulike metoder for å slette data på disse enhetene, vel vitende at samtlige enheter kan ha lagret kraftsensitiv informasjon. Hun lager en rutine som beskriver mulige slettemetoder: Spesiell programvare, avmagnetisering, knusing mv. og makulering av papirsøppel. Også utskrifter kan inneholde kraftsensitiv informasjon.

Sikkerhetsregler for mobile enheter

I bestemmelsen er det krav til å lage sikkerhetsregler for mobile enheter. Virksomhetene kan oppfylle kravet på følgende måte:

1. Lag regler for bruk av bærbare pc-er, mobiltelefoner, nettbrett og andre digitale enheter som kan motta, sende eller lese kraftsensitiv informasjon
2. Lage regler som dekker sikker bruk og oppbevaring, krav til autentisering, sikker oppkopling og overføring av data til server, sporing og sikker sletting av enhet ved tyveri og avhending
3. Sørg for at brukerne av de mobile enhetene er kjent med og har forstått reglene
4. La dokumentet som beskriver reglene være en del av internkontrollsystemet



Eksempel: Særskilte regler for beskyttelse av mobile enheter

Nett AS har gitt alle sine ansatte nettbrett og mobiltelefon. IKT-sikkerhetskoordinatoren har laget noen enkle sikkerhetsregler for bruk av disse. Det er for eksempel ikke tillatt å la andre låne nettbrettet og koden skal ikke deles med andre, heller ikke kollegaer. Enhetene blir sikkerhetsmessig administrert av Nett AS. Alle ansatte må gjennomgå en felles grunnopplæring i bruk og sikring av mobile enheter.



Standarder

- [NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav](#)

Veiledere

- [Digitaliseringsdirektoratet Internkontroll/styringssystem](#)

Krysskoplinger til annet regelverk

- § 2-5 Varsling og § 2-6 Rapportering
- § 2-10 Internkontrollsystem
- § 6-9 Digitale informasjonssystemer

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.

Ordforklaring

<i>Sikkerhetsinstruks</i>	Internt dokument i virksomheten som dokumenterer de viktigste interne prosedyrene for informasjonssikkerhet og beskyttelse av kraftsensitiv informasjon. Sikkerhetsinstruksen inngår i virksomhetens internkontrollsystem. Sikkerhetsinstruksen viser krav til hvordan man skal handle og opptre.
---------------------------	---

Hvordan oppfylle kravet

Virksomheten skal lage en sikkerhetsinstruks. Den må inngå i internkontrollsystemet. Første ledd omhandler krav til å utarbeide sikkerhetsinstruks.

- Sikkerhetsinstruksen bør angi ledelsens uttalte ambisjon eller målsetting for informasjonssikkerhet
- Sikkerhetsinstruksen må inneholde informasjon om hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll
Innholdet vil bero på hvilke tiltak virksomheten har iverksatt etter risikovurdering.
- Sikkerhetsinstruksen må stadfeste at leverandørers behandling av kraftsensitiv informasjon reguleres i sikkerhetsavtale med leverandøren

Andre ledd retter seg mot ansatte, der ansatte må ha en brukerinstruks for bruk av virksomhetens IT-systemer. Dokumentet må

- inneholde informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter *energilovens § 9-3 annet ledd*
- stille krav til undertegning av taushetserklæring
- inneholde informasjon om at kraftsensitiv informasjon ikke skal offentliggjøres

Sikkerhetsinstruksen kan bestå av ett eller flere dokumenter.



En brukerinstruks *bør* dekke følgende

- hvem instruksene gjelder for (eksempelvis ansatte og innleide konsulenter)
- hvilken verdi informasjon kan ha og krav til beskyttelse (eksempelvis offentlig, bedriftsintern, kraftsensitiv, personopplysninger)
- e-postbruk
- internettbruk
- sikkerhet på eget kontor, herunder passord, låsing av skjerm og ryddig pult
- lagring av informasjon administrert av virksomheten og sikkerhetskopiering
- utskrift, oppbevaring, kopiering og makulering av kraftsensitiv informasjon
- rutiner ved besøk og service
- rutine for låsing av kontor og aktivering av alarm
- fjerntilgang til virksomhetens systemer og IKT-tjenester
- sikkerhet ved bruk av mobile enheter
- sikkerhet på reise
- varsling av avvik og uønskede IKT-hendelser
- ansvarlig for dokumentet og siste revisjon



Maler

Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se [NVE maler](#)

NVEs mal for taushetserklæring på norsk og engelsk se [NVE maler](#)

Standarder

- [NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav](#)

Veiledere

- [Digitaliseringsdirektoratet Internkontroll/styringssystem](#)

Krysskoplinger til annet regelverk

- § 2-10. Internkontrollsystem
- § 6-9. Digitale informasjonssystemer
- § 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere
- § 6-3. Beskyttelse, avskjerming og tilgangskontroll
- § 6-5. Anskaffelser
- § 6-6. Begrenset anbudsinnbydelse

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.

Ordforklaring

<i>Revidere</i>	Se kritisk igjennom og foreta nødvendige rettelser og forandringer
<i>Påse</i>	Sørge for
<i>Driftskontrollsystemet</i>	Se § 7-1

Hvordan oppfylle kravet?

Bestemmelsen plasserer ansvaret for å sikre at leverandører etterlever kravene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon i KBO-enheten. Kravene kan oppfylles på følgende måte:

1. KBO-enhetene *må* i anskaffelsesdokumentene og i avtalen med leverandøren gjøre det tydelig at leverandøren er forpliktet til å beskytte kraftsensitiv informasjon og etterleve taushetsplikten. Se henvisning til mal nedenfor
2. KBO-enheten *må* i avtalen med leverandøren sørge for at de har rett til å kontrollere leverandørens etterlevelse av kravene til å beskytte kraftsensitiv informasjon. NVE godtar at etterlevelse kan sjekkes gjennom at KBO-enheten får innsyn i og sjekker tredjepartsrevisjonsrapporter av IKT-sikkerheten hos leverandøren
3. KBO-enheten *skal* ha rutiner for hvordan de følger opp leverandøren. KBO-enheten *kan* gjennomføre egen revisjon av leverandøren eller se gjennom og vurdere tredjeparts revisjonsrapporter om IKT-sikkerhet hos leverandøren. KBO-enheter som benytter samme leverandør, kan samarbeide om dette dersom det er hensiktsmessig

KBO-enheter trenger ikke inngå sikkerhetsavtale med andre KBO-enheter fordi disse allerede er underlagt forskriftens krav.



Eksempel: Leverandør går konkurs

Vannkraft AS har benyttet en IT-leverandør som behandler informasjon til et stort antall KBO-enheter. IT-leverandøren går konkurs, det blir oppnevnt bobestyrer og konkursboet blir raskt solgt til et annet selskap. Bobestyrer og deretter ny eier får dermed tilgang til kraftsensitiv informasjon. Digitale data er lagret på servere hos IT-leverandøren og dens underleverandør. Data som ikke i kontrakten er uttrykkelig eid av Vannkraft AS, inngår i konkursboet og er solgt.

IKT-sikkerhetskoordinatoren kontakter NVE for å be om råd. NVE ber ham sjekke eierskap til data og kontraktbetingelsene med vekt på sikring av kraftsensitiv informasjon. NVE tar videre kontakt med bobestyrer for å avklare spørsmål om hvordan kraftsensitiv informasjon er beskyttet, og hvem som har tilgang. NVE presiserer at *energilooven* § 9-3 om taushetsplikt gjelder for enhver, altså også konkursboet og bobestyrer. NVE informerer relevante aktører i KBO om hendelsen og gir samtidig råd om tiltak.



Eksempel: Leverandørrevisjon

Varmekraft AS har bestemt seg for å gjennomføre revisjon hos noen av sine leverandører. De velger ut en norsk IT-leverandør og en skytjeneste-leverandør. IKT-sikkerhetskoordinatoren tar kontakt med begge leverandørene og får avtalt revisjonsmøte med den norske IT-leverandøren. Skytjenesteleverandøren er et stort globalt selskap med kontor i Norge. IKT-sikkerhetskoordinatoren ber om å få se leverandørens revisjonsrapporter som er laget av uavhengige revisjonsfirma (tredjepartsrevisjon).

Maler



Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se [NVE maler](#)

NVEs mal for taushetserklæring på norsk og engelsk se [NVE maler](#)

Standarder

[NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav](#)

Veiledere

[Digitaliseringsdirektoratet Internkontroll/styringssystem](#)

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(norsk\)](#)

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(engelsk\)](#)

Krysskoplinger til annet regelverk

- § 2-10. Internkontrollsystem
- § 6-1. Identifisering av kraftsensitiv informasjon og rettmessige brukere
- § 6-2. Kraftsensitiv informasjon
- § 6-3. Beskyttelse, avskjerming og tilgangskontroll
- § 6-4. Informasjon om taushetsplikt i sikkerhetsinstruks og signering av taushetserklæring
- § 6-6. Begrenset anbudsinnbydelse
- § 6-9. Digitale informasjonssystemer

6.6 Begrenset anbudsinnbydelse

§

§ 6-6. Begrenset anbudsinnbydelse

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

Forståelsen av begrenset anbudsinnbydelse bygger på anskaffelsesregelverket.

Ordforklaring

<i>Sikkerhetsgradert informasjon</i>	Informasjon som kan skade nasjonale sikkerhetsinteresser dersom den blir kjent for uvedkommende, se. <i>sikkerhetsloven</i> § 5-3 Sikkerhetsgradert informasjon er underlagt taushetsplikt og er unntatt offentlighet iht. <i>sikkerhetsloven</i> § 5-4
<i>Anbudsdokumenter</i>	Alle dokumenter som tilgjengeliggjøres i anbudskonkurransen. Dette omfatter blant annet kunngjøringen, konkurransegrunnlaget og det europeiske egenerklæringsskjemaet, se. anskaffelsesforskriften § 4-2 bokstav b
<i>Anbudsinnbudelse</i>	Invitasjon til å delta i anbudskonkurranse

Hvordan oppfylle kravet?

Bestemmelsen pålegger KBO-enheten en plikt til å bruke begrenset anbudsinnbudelse når det er nødvendig for å forhindre at kraftsensitiv eller sikkerhetsgradert informasjon blir offentlig tilgjengelig.

Ved en åpen anbudsinnbudelse gjøres spesifikasjonene for anbudet alminnelig kjent og alle interesserte kan gi tilbud.

Ved begrenset anbudsinnbudelse kan alle interesserte leverandører levere forespørsel om å delta i konkurransen. KBO-enheten (oppdragsgiveren) skal først foreta en prekvalifisering, hvor KBO-enheten på bakgrunn av de innkomne forespørslene om deltakelse, vurderer om leverandørene oppfyller kvalifikasjonskravene KBO-enheten har satt. Bare de leverandørene som oppfyller kvalifikasjonskravene og deretter blir invitert av KBO-enheten til å delta i konkurransen, får innsyn i anbudsgrunnlaget. Leverandørene må først inngå sikkerhetsavtale med KBO-enheten.

KBO-enheten må gjøre innkjøperne i virksomheten oppmerksom på kravet til informasjonssikkerhet og regelverket for begrenset anbud.

1. KBO-enheten *må* vurdere om anbudsdokumentene inneholder sikkerhetsgradert eller kraftsensitiv informasjon.
Virksomheter som ikke er underlagt *sikkerhetsloven* og som ikke har mottatt sikkerhetsgradert informasjon (merket) fra andre virksomheter underlagt *sikkerhetsloven*, skal normalt ikke være i besittelse av sikkerhetsgradert informasjon. Sikkerhetsgradert informasjon skal være tydelig merket i henhold til *sikkerhetslovens* bestemmelser.
2. Hvis anbudsdokumentene inneholder kraftsensitiv eller sikkerhetsgradert informasjon, må KBO-enheten velge begrenset anbudsinnbudelse. Dette betyr at det kun er leverandører som er prekvalifisert og har inngått sikkerhetsavtale med KBO-enheten som får tilsendt anbudsdokumentene.



Eksempel: Begrenset anbudsinnbydelse

Kraftkonsernet AS skal anskaffe nytt vedlikeholdssystem. Kraftsensitiv informasjon skal beskyttes. IKT-sikkerhetskoordinatoren diskuterer saken med innkjøpsansvarlig i virksomheten, som argumenterer for at åpne anbud gir lavest pris.

IKT-sikkerhetskoordinatoren påpeker at kraftsensitiv informasjon vil bli offentliggjort i anbudsprosessen. Kraftberedskapsforskriften gir mulighet til begrenset anbudsinnbydelse. Det blir besluttet å gjennomføre en prekvalifiseringsprosess der krav til sikkerhet inngår i betingelsene for å få tilsendt anbudsdokumentene. IKT-sikkerhetskoordinatoren bruker NVEs sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning, i tillegg til aktuelle veiledere fra Nasjonal sikkerhetsmyndighet (NSM). Så starter arbeidet med å utarbeide prekvalifiseringskrav.



Maler

Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se [NVE maler](#)

NVEs mal for taushetserklæring på norsk og engelsk se [NVE maler](#)

Standarder

Veiledere

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(norsk\)](#)

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(engelsk\)](#)

[Veiledning til reglene om offentlige anskaffelser \(anskaffelsesforskriften\)](#)

[Begrenset anbudskonkurranse, Regjeringen 2017](#)

[Veiledning i håndtering og beskyttelse av sikkerhetsgradert informasjon](#)

Krysskoplinger til annet regelverk

- § 2-10. Internkontrollsystem
- § 6-4. Sikkerhetsinstruks
- § 6-5. Anskaffelser
- [Forskrift om offentlige anskaffelser \(anskaffelsesforskriften\)](#) .
- [Lov om nasjonal sikkerhet \(sikkerhetsloven\)](#)

6.7. Personkontroll



OBS! NVE legger ny tolkning til grunn. Personkontroll utøves ved bakgrunnssjekk ved ansettelse, og gjennom personalpolitikk og tilgangsstyring gjennom hele ansettelsesforholdet. KBO-enhetene kan gjennomføre kredittsjekk når det er saklig behov for det iht. personopplysningsforskriftens § 4-3. NVE anbefaler at KBO styrer innsiderisiko gjennom andre sikringstiltak, eksempelvis vurdering av landrisiko ved ansettelse, personalpolitikk og tilgangskontroll gjennom hele ansettelsesforholdet.



§ 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.

Ordforklaringer

<i>Bakgrunnssjekk</i>	Bakgrunnssjekk er prosessen med å innhente, sammenligne og dokumentere informasjon om en person for å bekrefte eller avkrefte det personen selv opplyser. Bakgrunnssjekk består av identitetskontroll, verifisering av utdanning og arbeidserfaring, søk i adresseregistre og andre åpne kilder, sjekk av næringsinteresser og eventuelt kredittsjekk. Full bakgrunnssjekk vil si at alle ovennevnte elementer inngår; merk at kredittsjekk ikke er nødvendig i full bakgrunnssjekk.
<i>Egnethetsvurdering</i>	Helhetsvurdering av om en person er egnet for tilsetting eller tilgang, basert på funn fra bakgrunnssjekken
<i>Kredittsjekk</i>	Kontroll og vurdering av kredittverdigheten og betalingsevnen for en person. Kredittsjekk er en tjeneste som selges av kredittopplysningsbyråer, og er det samme som kredittvurdering.

Hvordan oppfylle kravet

Formålet med bestemmelsen er å bidra til å sikre klassifiserte anlegg og system mot innsiderisiko. Bestemmelsen gjelder kun KBO-enheter og kun nyansatte og egne ansatte som har fått ny stilling. Risikofaktorer som taler imot egnethet, er mangelfull holdning til sikkerhet, misnøye, ustabil adferd, kontakt med kriminelle enkeltpersoner eller miljøer, indikasjoner på rusmisbruk, økonomiske problemer eller overdrevent forbruk i forhold til inntekt og formue. Holdninger og uavklarte forhold fra bakgrunnssjekken bør søkes avklart ved intervju med den aktuelle personen.

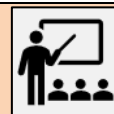
Personopplysninger som behandles i forbindelse med egnethetsvurderingen, skal slettes så fort formålet med innhentingen er oppfylt. Opplysninger fra kredittsjekk skal slettes når egnethetsvurderingen er gjennomført. Behandling av personopplysninger må gjøres i samsvar med *personvernloven*. NVE viser til Datatilsynet for veiledning. NVE viser ellers til veilederen "Sikkerhet ved ansettelsesforhold, før, under og ved avvikling, utgitt av Politiets sikkerhetstjeneste", Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd.

KBO-enheter kan kreve at personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3, skal fremlegge kredittsjekk, men **kun når det er saklig behov for det iht. personopplysningsforskriftens § 4-3. I praksis betyr dette at kredittsjekk kun kan gjøres når vedkommende skal kunne ta opp kreditt eller ha økonomiansvar som en del av stillingen sin.** NVE anbefaler derfor at virksomheten har god opplæring av ansatte, gode rutiner for tilgangskontroll til IKT-systemer og en personalpolitikk som bygger tillit og lojalitet til virksomheten, og som gir trygghet for å rapportere uønskede hendelser. NVE anbefaler videre at man vurderer landrisiko ved ansettelse og innleie av personell fra utlandet og følger råd gitt fra sikkerhetsmyndighetene (PST, Forsvaret og NSM).

For fysisk adgang til driftssentraler i klasse 3 gjelder et absolutt krav om full bakgrunnssjekk, se kbf § 5-11. Dette gjelder alle personer som skal ha slik adgang, interne og eksterne.

NVE anbefaler at KBO-enheter har på plass sikringstiltak, tilgangskontroll og god personalledelse i hele ansettelsesperioden.

Kravene gjelder ikke personer som er klarert og autorisert i henhold til *sikkerhetsloven*. Dette gjelder både sikkerhetsklarering og adgangsklarering. For sivil sektor er Sivil klareringsmyndighet (SKM) den sentrale klareringsmyndigheten.



Eksempel: Personkontroll av ansatte

Kraftkonsernet AS skal ansette en ny økonomisjef g med fullmakt til å foreta økonomiske transaksjoner, herunder handle på kreditt på vegne av virksomheten. Medarbeideren vil få tilgang til anlegg i klasse 2 og 3. Bakgrunnssjekk av nyansatte innebærer for eksempel kontroll av identitet, framvisning av originalvitnemål, verifikasjon av kompetanse og erfaring gjennom intervju og referansesjekk. I tillegg kan Kraftkonsernet AS gjennomføre kredittsjekk av den nye økonomisjefen.

I denne ansettelsessaken har det dukket opp spørsmål om Kraftkonsernet AS må gjennomføre bakgrunnssjekk av alle ansatte i virksomheten. I samtale med NVE kommer det frem at dette kravet kun gjelder for nyansatte. Det kan også unntaksvis gjelde for egne ansatte, dersom de har fått en *ny stilling*, for eksempel går fra vedlikeholdsavdelingen til driftssentralen. Kraftkonsernet AS skal gjennomføre personkontroll av alle, inklusive ansatte hos leverandører, når de skal ha fysisk selvstendig adgang til driftssentral klasse 3. Dette kravet følger av § 5-11. Dette kravet sier at personer uten full bakgrunnssjekk etter § 6-7 ikke skal ha adgang til driftssentraler i klasse 3.

Kraftkonsernet AS skal også ansette en tekniker som skal jobbe i anlegg i klasse 2 og 3. Han skal også jobbe på driftssentralen. I dette tilfellet skal Kraftkonsernet gjennomføre full bakgrunnssjekk før ansettelse. Han har ikke budsjettansvar eller økonomifullmakt, og det er ikke saklig behov for kredittsjekk etter personopplysningsforskriften § 4-3. Følgelig skal kredittsjekk ikke gjøres.



Personkontroll av ansatte hos leverandører og andre aktører som må ha tilgang

Kraftkonsernets anlegg i klasse 2 og 3 er samlokalisert med teleanlegg. Teleselskapets servicepersonell trenger derfor adgang til anlegget for å få adgang til eget utstyr. Teleselskapets personell får dermed adgang til anlegg i klasse 2 og 3 som tilhører Kraftkonsernet. Kraftkonsernet henvender seg til NVE med forespørsel om hvordan hjemmelen for personkontroll er for Teleselskapets personell. NVE forklarer at Kraftkonsernet ikke har hjemmel til å kreve personkontroll med unntak av for det servicepersonellet som skal inn på driftssentralen i klasse 3.

NVE godtar at Teleselskapet «går god» for sine ansatte, dvs. servicepersonellet. I dette tilfellet skal det foreligge en liste over godkjent personell.



Veiledere

[Sikkerhet ved ansettelsesforhold, før, under og ved avvikling, utgitt av Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd](#)

[Kredittvurdering, Datatilsynet](#)

[NSM Risiko 2022.pdf](#)

[Nasjonal trusselvurdering - 2022 \(pst.no\)](#)

[Fokus 2022 - Forsvaret](#)

Krysskoplinger til annet regelverk

[5-11 Restriksjoner for adgang til steder og områder](#)

[§ 6-4 Sikkerhetsinstruks](#)

[§ 6-9 Digitale informasjonssystemer](#)

[§ 7-2 Interne sikkerhetsregler](#)

[§ 7-4 Kontroll med brukertilgang](#)

[Lover og regler, Datatilsynet](#)

6.8 Sikkerhetskopier



§ 6-8. Sikkerhetskopier

Virksomheter skal ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet som er av betydning for drift, sikkerhet og gjenoppbygging av kraftforsyningen. Sikkerhetskopiene skal fjernlagres på et sikkert sted, som er lett tilgjengelig for virksomheten.

Nødvendig dokumentasjon om energisystemet og som lagres på datamedia, skal også foreligge som papirutskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted som er lett tilgjengelig for virksomheten.

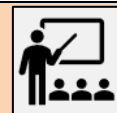
Hvordan oppfylle kravet

Første ledd handler om systemgjenoppbygging (driftskontrollsystem). Digital sikkerhetskopi er godt nok så lenge denne sikkerhetskopien alltid er tilgjengelig uavhengig av skytjeneste- eller IT-leverandørens oppetid og kvalitet på sine systemer (dvs. at tilgjengelighet og integritet er sikret). I praksis bør det derfor finnes lokalt lagrede sikkerhetskopier der virksomheten også har testet at kopiene fungerer. Virksomheter må

- ha oppdaterte sikkerhetskopier av nødvendig informasjon, programvare og konfigurasjoner av driftskontrollsystemet
- fjernlagre sikkerhetskopi på sikkert sted som er lett tilgjengelig for virksomheten
- beskytte sikkerhetskopier i henhold til kravene i § 6-9
- ha offline sikkerhetskopi

Annet ledd handler om beredskap for manuell drift. Papirkopikravet gjelder energisystemet. Formålet er å sikre at virksomheten evner å reparere feil i nettet og få gjenoppbygget energiforsyningen selv i de situasjoner der digitale systemer kan svikte. Virksomheten må derfor

- lagre og årlig oppdatere nødvendig dokumentasjon om energisystemet på datamedia og på papir og oppbevare dette på et sikkert og for virksomheten lett tilgjengelig sted. Hva som er nødvendig dokumentasjon, må skjønnsmessig vurderes av virksomheten
- oppbevare sikkerhetskopien slik at ikke samme hendelse ødelegger original og kopi



Eksempel: Sikkerhetskopier av driftskontrollsystemet

«Ikke koble PC og nettbrett på nettet – vi er utsatt for cyberangrep!»

Denne meldingen gikk ut på SMS til alle ansatte i Kraftkonsernet AS. Økonomisystemet var blant de systemene som ble rammet. Angriperen krevde betalt i kryptovaluta og truet med å publisere sensitive data. Beredskapsplanene fantes heldigvis i sikkerhetskopi på andre datamedia og på papir, sikret og adskilt fra de systemene som var rammet. Kraftkonsernet AS hadde tidligere i år gjennomført øvelse og testet at systemet kunne gjenopprettes med sikkerhetskopien som var lagret offline. Å betale utpressingspenger er sterkt frarådet siden slik utbetaling støtter kriminell virksomhet og viser at virksomheten vil betale for å få dekrypteringsnøkkelen. Å ikke betale for utpressingen og ha en beskyttet og testet sikkerhetskopi er derfor en god forebyggende sikring mot følgene av slike utpressingsangrep.

Virksomheten bør

- plassere tydelig ansvar i organisasjonen for å vurdere behovet for sikkerhetskopier og gjenoppretting av samtlige IT-tjenester
- ha en backup-plan og utføre nødvendige tester
- vedlikeholde og oppdatere et dokument som beskriver ansvar og roller, samt prosedyrer for sikkerhetskopi/gjenoppretting. Sikkerhetskopi/gjenoppretting må ta hensyn til betydningen av å ha tilgang til informasjon og behovet for oppetid for systemene
- vurdere om leverandørers innebygde funksjonalitet for backup og muligheter for å hente sikkerhetslagrede data er gode nok, eller om virksomheten må lage egen rutine for sikkerhetskopi/gjenoppretting. Sikkerhetskopi/gjenoppretting for nye tjenester må vurderes fortløpende
- lagre original og sikkerhetskopi på to ulike fysiske steder for å unngå at samme hendelse, eksempelvis brann eller flom, ødelegger begge
- lagre papirkopier av nødvendig digitalisert dokumentasjon om energisystemet på to ulike fysiske steder. Eksempel er enlinjeskjemaer, beredskapsplaner og innsatsplaner, oversikt/kontaktliste over leverandører samt nødvendig oversikt over infrastrukturen



Veileder

[NSM og KRIPOS, 2020, Løsepengevirus temarapport](#)

Standarder

ISO/IEC 270140 Information Technology – Security Techniques – Storage security gir ytterligere veiledning på datalagringssikkerhet (Publisert 2015-01).

Krysskoplinger til annet regelverk

- § 2-5. Beredskapsplanlegging
- § 6-9. Digitale informasjonssystemer

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

Ordforklaring

Digitale informasjonssystemer	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 tilgang for rettmessige brukere.
Verdi	Med verdi menes virksomhetens leveranser av for eksempel elektrisk energi og fjernvarme, tjenester og produkter. Verdier er også anleggsmidler og informasjon inklusive intellektuelle rettigheter. Listen er ikke prioritert eller uttømmende.
Sikringstiltak	Tiltak for å redusere risiko forbundet med uønskede handlinger
Risikovurdering	Se § 2-3
Sektorvist responsmiljø	Se § 3-6
Uønsket hendelse	Uønskede hendelser omfatter både tilsiktede handlinger og utilsiktede hendelser. Begge deler kan påvirke sikkerhetsverdiene konfidensialitet, integritet og tilgjengelighet. Uønskede hendelser kan gi opphav til ekstraordinære situasjoner.
Hendelseshåndtering	Aktiviteter med formål om å stanse eller begrense skade av uønskede hendelser på berørte IKT-systemer og nettverksressurser, og deretter gjenopprette sikker tilstand.
Tjenesteutsetting	Ekstern utførelse av basisdrift, applikasjonsdrift eller applikasjonsforvaltning med en tjenesteleverandør. Tjenesteutsetting (outsourcing), utkontraktering og konkurranseutsetting er likeverdige betegnelser
Sikkerhetsrevisjon	Virksomhetens interne og eksterne kontroll av eget sikkerhetsarbeid.

Hvordan oppfylle kravet

Kbf § 6-9 plasserer ansvaret for digital sikkerhet i virksomheten. I tillegg detaljeres krav til grunnsikring. Kravene bygger på NSMs grunnprinsipper for IKT-sikkerhet. NSMs grunnprinsipper for IKT-sikkerhet bygger igjen på internasjonale anerkjente standarder og veiledninger, spesielt ISO/IEC 27002. NSM har på sin nettside om grunnprinsippene laget en oversikt over hvordan grunnprinsippene samsvarer med ISO 27002. NSM har også gitt ut grunnprinsipper for sikkerhetsstyring.



Internasjonale standarder og veiledning for ytterligere kunnskap

- ISO/IEC 27000 serien (foretrukket i EU)
- Cyber Essentials (NCSC, UK)
- NIST Cyber Security Framework (USA)
- Center for Internet Security CIS CSC Top 20 Security controls, Risk Assessment Templates og Benchmarking verktøy
- Cloud Security Alliance standard

Grunnprinsippene forteller hva du må gjøre, men ikke hvordan. Hvert grunnprinsipp beskriver en kontinuerlig aktivitet som må gjennomføres og 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 gjennomføres effektivt. NSM har derfor kategorisert grunnprinsippene i tre kategorier, 1, 2 og 3, der man starter med kategori 1 tiltak. I sum inkluderer grunnprinsippene bredden av sikringstiltak som består av barrierer, deteksjon, verifikasjon og reaksjon for å etablere god sikkerhet i dybden.

NVE anbefaler virksomheter å sette seg inn i NSMs grunnprinsipper for IKT-sikkerhet og NSMs grunnprinsipper for sikkerhetsstyring. Mer detaljerte råd om konfigurasjon og teknisk sikkerhet gis av Center for Internet Security. Også standarder er nyttige kilder til mer informasjon. De har ofte mye felles, og man kan velge den som passer virksomheten best, og supplere med tiltak fra andre rammeverk om man ønsker det.

Som et minimum bør virksomhetene tilstrebe å ha et sikkerhetsnivå tilsvarende kategori 1 og 2 tiltak. For større virksomheter kommer i praksis alle grunnprinsippene under de ulike hovedkategoriene til anvendelse. Nedenfor følger en gjennomgang av *kravene* i bokstav a til f.

Virksomheten skal ha en grunnsikring for digitale informasjonssystemer i henhold til anerkjente standarder og normer. Her vektlegger kravet at virksomheten bør se til standarder og normer for sikring av digitale systemer.

a. Identifisere og dokumentere

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

Aktiviteten er grunnlaget for effektiv innføring 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:

- 1.1 kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 kartlegg enheter (inventar) og programvare
- 1.3 kartlegg brukere og behov for tilgang

NVE anbefaler i tillegg at normal nettverkstrafikk kartlegges.

Dokumentasjonen skal holdes oppdatert. Det innebærer at virksomheten må ha prosedyre og system som sørger for oppdatering og at endringer blir registrert.

Store virksomheter og virksomheter med klasse 2 og klasse 3 driftskontrollsystem bør iverksette samtlige grunnprinsipper og tilhørende tiltak. Alle virksomheter må iverksette kategori 1 og 2 tiltak – dette utgjør totalt 35 tiltak.

b. Risikovurdering

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

Risiko skal generelt vurderes for både konfidensialitet, integritet og tilgjengelighet. Risikovurderinger kan ha ulik oppløsning og innretning. Se § 2-3. *Risikovurdering*. Direktoratet for IKT og fellestjenester i høyere utdanning og forskning har utviklet veiledere for risikovurdering av IKT-sikkerhet i administrative systemer og i skytjenester. De viser hvordan en risikovurdering av administrative systemer og skytjenester kan gjøres.

Større virksomheter og virksomheter med klassifiserte driftskontrollssystemer bør følge en anerkjent standard, veiledning eller norm for risikovurdering. NVE gir ikke føringer for hvilken metode, norm eller rammeverk som skal brukes. NVE viser til § 2-3 og understreker at risikovurderingens hensikt er å styre risiko slik at virksomheten velger de rette tiltakene og reduserer risikoen til et akseptabelt nivå.



Eksempel: Enkel risikovurdering av mindre endring i IT-systemet

Virksomhetens IKT-sikkerhetskoordinator skal gjøre en mindre endring i IT-systemet. En enkel risikovurdering kan ta utgangspunkt i en avgrenset del av IT-systemet eller en viktig tjeneste/applikasjon. Innenfor IKT-sikkerhet er det enkelt forklart tre uønskede hendelser som kan inntreffe:

1. Systemet blir utilgjengelig
2. Systemets funksjonalitet (programvare) blir endret og integriteten skades
3. Informasjonslekkasje av kraftsensitiv informasjon

Hva er årsakene til at dette IT- systemet eller IT-tjenesten blir utilgjengelig?
Det kan være mange årsaker med ulik grad av sannsynlighet: Overbelastning av datatrafikk, infeksjon med kryptoskadevare, ordinær oppdatering av programvare som fører til at kommunikasjon med annen IT-tjeneste ikke fungerer, lisensen har gått ut, strømbrudd, brudd på kommunikasjonslinjer utenfor virksomheten, med flere.

Neste trinn er en skjønnsmessig vurdering av sannsynligheten for at årsakene kan inntreffe.

Videre må det vurderes hva man kan gjøre for å fjerne årsakene. Ulike barrierer som oppdatering av programvare, brannmur (nettverkstrafikkontroll), styring av tilgang og brukerrettigheter, og redundante systemer er barrierer som kan forebygge en rekke årsaker til nedetid. Det finnes flere barrierer.

Om ikke hendelsen kan unngås, hva er konsekvensene for virksomheten? Hvordan kan konsekvensen reduseres? Kan beredskapsplan og innsatsplaner bidra til å redusere konsekvensene? Kan forberedte tiltak som beskyttet og testet sikkerhetskopi redusere konsekvensene av hendelser? Eller er konsekvensen minimal i form av nedetid, rettelarbeid og tidsbruk, og kan håndteres av IT-drift dersom den inntreffer?

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 (se kbf § 6-2), bedriftshemmeligheter, personopplysninger (se *personopplysningsloven*) eller gradert informasjon (se *sikkerhetsloven*). Annen informasjon vil være åpen informasjon.

I kravet til å sikre inngår følgende grunnprinsipper

- 2.1 ivareta sikkerhet i anskaffelses- og utviklingsprosesser
- 2.2 ivareta en sikker IKT-arkitektur
- 2.3 ivareta en sikker konfigurasjon (av maskin- og programvare)
- 2.4 beskytt virksomhetens datanettverk
- 2.5 kontroller dataflyt
- 2.6 ha kontroll på identiteter og tilganger
- 2.7 beskytt data i ro og i transitt
- 2.8 beskytt e-post og nettleser
- 2.9 etablere evne til gjenoppretting av data
- 2.10 integrer sikkerhet i prosess for endringshåndtering

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 og logge endringer

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

I kravet til å oppdage inngår følgende grunnprinsipper:

- 3.1 oppdag og fjern kjente sårbarheter og trusler
- 3.2 etabler sikkerhetsovervåkning
- 3.3 analyser data fra sikkerhetsovervåkning
- 3.4 gjennomfør inntrengningstester

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

Virksomheten skal varsle uønskede hendelser som for eksempel datainnbrudd, nektelsesangrep, oppdagelse av skadevare eller sabotasjeforsøk til det sektorvise responsmiljøet. KraftCERT skal motta alle varsler på uønskede IKT-hendelser. Når virksomhetene er flinke til å varsle til KraftCERT, er det lettere å lage et situasjonsbilde over trusselsituasjonen i bransjen. Et oppdatert situasjonsbilde er nyttig for å treffe med sikringstiltak og beredskap. I tillegg skal ekstraordinære situasjoner varsles til beredskapsmyndigheten (NVE) uten ugrunnet opphold, se § 2-5 og uønskede hendelser skal rapporteres til NVE, se § 2-6.



Eksempel; Varsling av datainnbrudd

Nett AS sine IT-systemer blir, som andre virksomheters IT-systemer, stadig utsatt for portscanning og inntrengingsforsøk. IKT-sikkerhetskoordinatoren har egentlig altfor mye å gjøre, slik at en sårbarhet som har vært varslet av KraftCERT for flere uker siden, har dessverre ikke blitt lukket. Som en del av en angrepskampanje mot selskap i energisektoren, ble derfor også Nett AS utsatt for datainnbrudd i sitt administrative IT-system.

IKT-sikkerhetskoordinatoren varslet KraftCERT om denne hendelsen. KraftCERT rådet ham å ta kontakt med tekniske spesialister som kunne bistå. IKT-sikkerhetskoordinatoren varslet også NVE ettersom kbf § 2-5 stiller krav om varsling ved innbrudd. Innbrudd skjer ikke bare i bygg, men også i datasystem.

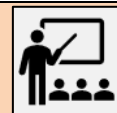
d. Håndtere og gjenopprette

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

Virksomheten må ha system, prosedyre og plan for å håndtere sikkerhetsbrudd og gjenopprette systemer og data når systemene feiler. Til hendelseshåndtering hører også vurdering av skadeomfang, begrense skadeomfanget, sikre bevis, skaffe bistand og eksperthjelp, og varsle og rapportere som forskriften krever. Tiltak og aktiviteter bør dokumenteres underveis, mens evaluering, læring og forbedring er del av oppfølgingen i etterkant av hendelsen. Følgende grunnprinsipper inngår:

- 4.1 forbered virksomheten på håndtering av hendelser
- 4.2 vurder og klassifiser hendelser
- 4.3 kontroller og håndter hendelser
- 4.4 evaluer og lær av hendelser

For anskaffelse av tjenesteleverandør til hendelseshåndtering og etterforskning i systemene henviser NVE til NSMs kvalitetsordning for leverandører.



Eksempel: Rapportering av hendelse til NVE

Etter flere uker med etterforskning og gjenoppretingsarbeid er Nett AS sine administrative systemer igjen i full drift. Nett AS har i denne perioden samarbeidet med KraftCERT, ulike leverandører og spesialister. Utgiftene til konsulentbistand og gjenoppretting har vært store, og nå har Nett AS rimelig god oversikt over hendelsesforløpet. Nett AS sender inn en rapport om hendelsen til NVE.

e. Tjenesteutsetting

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

Virksomheten må ha tilstrekkelig kompetanse om anskaffelse og IKT-sikkerhet. Kompetente rådgivere må hentes inn eksternt dersom virksomheten selv mangler tilstrekkelig kompetanse. Sikkerhet må tas hensyn til tidlig i prosessen mens virksomhetene enda har forhandlingsrom og påvirkningsmulighet.

Virksomheten må dokumentere det eksisterende systemet og sikkerhetsnivået, før virksomheten går i gang med tjenesteutsetting. Dokumentasjonen må være så detaljert at det er mulig å kontrollere endringer i sikkerhetsnivå, 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.

IT-industrien er global og benytter underleverandører spredt over hele verden. Virksomheter som planlegger tjenesteutsetting, har derfor behov for å vurdere landrisiko for å sørge for at sikkerhetsnivået opprettholdes. Garantikassen for eksportkreditt (GIEK) har en nettside med samlet vurdering av landrisiko for alle land i verden, og NSM har utarbeidet en veileder for landrisikovurdering. For tjenesteutsetting av IKT-systemer som behandler kraftsensitiv informasjon (se. § 6-2), gjelder særlige hensyn for å sikre at taushetsplikten ivaretas. Se også NVEs sjekkliste for IKT-sikkerhet og NSMs veileder for tjenesteutsetting. Aktuelle leverandører bør være sertifisert i henhold til én eller flere internasjonalt anerkjente sikkerhetsstandarter. 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 av IKT-drift:

- dokumentere eksisterende system (se. §6-9 a) og organisasjonens IKT-sikkerhetskompetanse
- 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)
- innføre og forvalte ny løsning, og bygge opp nødvendig kompetanse

- dokumentere nytt system/tjenestemodell, se. § 6-9 a og ivareta behov for tilgang til IKT-sikkerhetskompentanse
- overføre kunnskap fra tidligere leverandør til ny leverandør, avslutte eksisterende løsning(er) og sørge for at kraftsensitiv informasjon er slettet hos tidligere leverandør



Eksempel: Tjenesteutsetting

Ledelsen vurderer å tjenesteutsette drift av all administrativ IT. IKT-sikkerhetskoordinatoren ser at forskriften stiller krav til at sikkerhetsnivået må opprettholdes eller forbedres. Han må kunne dokumentere at sikkerheten er minst like god etter tjenesteutsettingen. Det betyr at han må ha god oversikt og dokumentasjon av aktuelle systemer, samt risiko og hendelsesstatistikk. Dette kan han sammenholde med ny løsning når denne har vært i drift en stund. Han benytter «NVEs sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen» som veiledning.



Ikke undervurder behovet for egen intern kompetanse ved tjenesteutsetting

Virksomheten må ta høyde for å ha kompetanse og kapasitet til å utvikle gode kravspesifikasjoner, følge opp leverandører i drift og ved overgang til nye driftsleverandører.

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.

Revisjon av iverksatte sikringstiltak for digitale informasjonssystemer skal være en gjentakende aktivitet. Som minimum må revisjonen kontrollere organisering av sikkerhetsarbeidet, inkludert plassering av ansvar, og tiltak for å beskytte kraftsensitiv informasjon mot uautorisert tilgang. Revisjon av systemer som er driftet av ekstern leverandør, kan omfatte kontroll av tredjepartsrevisjonsrapport og -sertifiseringer. Resultatene og konklusjonene fra sikkerhetsrevisjonene må dokumenteres. Avvik og feil må håndteres i henhold til virksomhetens internkontrollsystem, kbf § 2-10. NVE krever ikke at alle leverandører skal revideres årlig, men virksomheten må gjøre et valg av leverandører basert på risiko og vesentlighet. Revisjonsrapporter må være et tema i virksomhetens ledermøter eller andre relevante fora i virksomheten.



Veiledere

[NIST Guide for Conducting Risk Assessment](#)

[Risikostyring av IKT-sikkerhet i leverandørkjeder](#)

[NSM Grunnprinsipper i sikkerhetsstyring](#)

[Digdir Helhetlig styring og kontroll av informasjonssikkerhet](#)

[NSM grunnprinsipper for IKT-sikkerhet 2.0](#)

[Kvalitetsordning for leverandører som håndterer IKT-hendelser, NSM](#)

[Landvurdering ved tjenesteutsetting av IKT-tjenester - Nasjonal sikkerhetsmyndighet \(nsm.no\)](#)

[Garantikassen for eksportkreditt – landrisikovurdering](#)

[Sikkerhetsfaglige anbefalinger ved tjenesteutsetting, NSM \(/2020\)](#)

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(norsk\)](#)

[Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning \(engelsk\)](#)

[Metode for å finne kraftsensitiv informasjon på internett](#)

[Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon](#)

[Nettvett, Sikker sletting](#)

[Digdir Veileder for testing av etterlevelse av sikkerhetsstandarder](#)

[Tiltak mot skadevare og løsepengevirus, NSM \(2021\)](#)

[CIS Benchmarks - konfigurasjonsråd for mange produkter](#)

[Sikkerhetsveileder for kraftsensitiv informasjon i skytjenester, FSK \(november 2021\).](#)

[Risikovurdering av IKT-systemer.pdf \(nsm.no\)](#)

[Vedlegg- Mal for risikovurdring IKT-systemer.xlsx \(live.com\)](#)

Standarder

- ISO/IEC 27001: 2017
- ISO/IEC 27002: 2017
- NIST Cyber Security Framework

Krysskoplinger til annet regelverk

- § 2-3. Risikovurdering
- § 2-4. Beredskapsplanlegging
- § 2-5. Varsling
- § 2-6. Rapportering
- § 2-7. Øvelser
- § 2-9. Evaluering
- § 2-10. Internkontrollsystem
- § 6-5. Anskaffelser
- § 6-6. Begrenset anbudsinnbydelse

6.10 Beskyttelse av 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 netjtjenester 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.

Ordforklaringer

Ord	Forklaring
Avanserte måle- og styringssystem (AMS)	AMS er et informasjons- og kommunikasjonssystem for avregning av utveksling, innmating og uttak, fra og med elektrisitetsmålerne til og med sentralsystemet hos nettselskapet eller nettselskapets leverandør.
Brytefunksjonalitet	System for fjernstyrt inn- og utkobling av strømuttaket i målepunktet til AMS-målere.
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 er og har vært inne i sonen.

<i>Fjerntilgang</i>	Tilgang til IKT-system fra en fysisk lokalitet utenfor anlegget der IKT-systemets maskinvare befinner seg.
<i>Fjernstyring</i>	Styring som skjer over en geografisk avstand.
<i>Kontrollordninger</i>	Tekniske sikkerhetstiltak, sikkerhetsmekanismer og prosedyrer.

Hvordan oppfylle kravet

Bestemmelsen gjelder for nettselskap som har AMS med brytefunksjonalitet.

AMS er et digitalt informasjonssystem og kravene til grunnsikring i § 6-9 gjelder derfor også for sikring av den logiske kjeden og kommandoer fra virksomhetens sentralsystem gjennom nettverket og fram til brytefunksjonen i måleren.

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

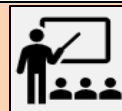
Det er ingen andre enn nettselskap som kan kople bryteren i AMS-målerne. Leverandøren av AMS-systemet har ikke denne tillatelsen. Fjernstyring må skje fra en adgangskontrollert sone, se § 5-1, der det er fysisk kontroll med hvem som har adgang, og der kun personell med legitimt behov har adgang. For eksempel vil ikke et hotellrom være adgangskontrollert sone fordi en ikke har kontroll over hvem som besøker et slikt rom.

- 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 som gjelder for driftskontrollsystemer.

Dersom nettselskapet har behov for å gi leverandører utenfor EFTA, EU eller NATO tilgang til AMS, må selskapet gjøre en landrisikovurdering og iverksette nødvendige sikringstiltak. Se punkt § 6-10 e. 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.



Eksempel: AMS-drift fra utlandet

Nett AS har installert AMS-målere hos sine kunder. Leverandøren av målerne har bestemt å flytte all sin virksomhet ut av Europa. Nett AS er pålagt å gjøre en risikovurdering som inkluderer landrisiko når leverandøren befinner seg utenfor Europa. Risikoen kan håndteres ved hjelp av forebyggende sikringstiltak (barrierer) og eller konsekvensreduserende tiltak (beredskap). Nett AS har uansett plikt til å ha barrierer på plass som hindrer at en enkelt bruker kan kople ut flere målere samtidig.

Nett AS er forpliktet til selv å ha oppsyn av leverandøren, mens denne har tidsbegrenset fjerntilgang. Han kan alternativt engasjere en tredjepart lokalisert i Norge, eller i et land i EFTA, EU eller NATO, som gjør denne jobben på vegne av Nett AS. Drift og vedlikehold av AMS fra utlandet blir tema på neste ledermøte i Nett AS.

- 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 og soneinndeling
- separering av rettigheter (privilegier)
- flerfaktor-autentisering for brukere
- logging og etterkontroll av logger kontinuerlig
- reaksjoner på brudd på rutinene som for eksempel sikkerhetssamtale eller avtaleoppsigelse

- 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.*

Dette kravet kommer i tillegg til sikring av digitale informasjonssystemer, se 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 andre AMS-målere. Hver måler må derfor ha innebygget sikkerhetsløsning som forhindrer at brytefunksjonaliteten blir misbrukt og at for eksempel skadevare forplanter seg fra en måler til en annen.



Veiledere

[RME Veileder nr 1/2022. Veileder til sikkerhet i AMS](#)

[NIST Guidelines for Smart Grid Cybersecurity](#)

Krysskoplinger til annet regelverk

- § 2-10 Internkontrollsystem
- § 5-1 Sikringsplikt
- § 6-9 Digitale informasjonssystemer
- [Forskrift om måling, avregning, fakturering av nettenester og elektrisk energi, nettselskapets nøytralitet mv.](#) se § 1-3

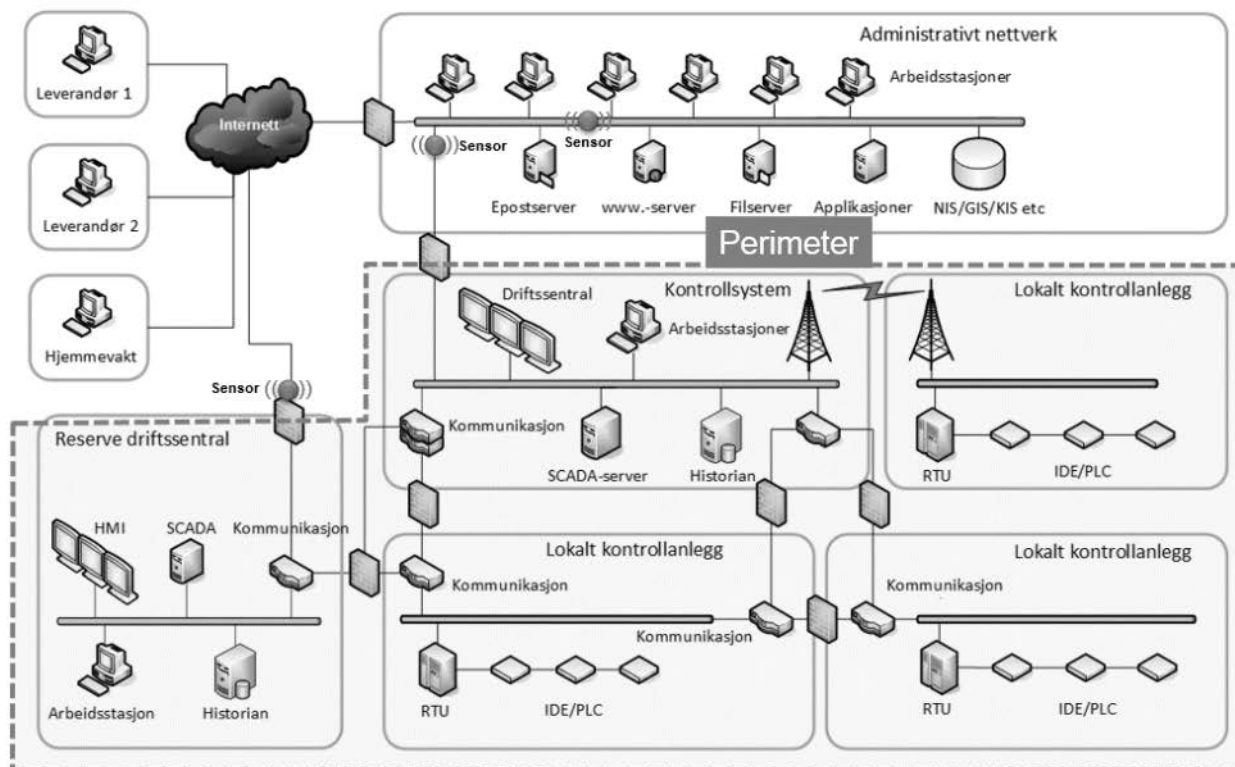
Innhold

7. Beskyttelse av driftskontrollsystem	1
7.1 Generell plikt til å beskytte driftskontrollsystemet	3
7.2 Interne sikkerhetsregler	6
7.3 Dokumentasjon av driftskontrollsystemet	8
7.4 Kontroll med brukertilgang	11
7.5 Kontroll ved endringer i driftskontrollsystemet	14
7.6 Kontroll med utstyr i driftskontrollsystemet	16
7.7 Håndtering av feil, sårbarheter og sikkerhetsbrudd	19
7.8 Beredskap ved svikt i driftskontrollsystemet	21
7.9 Bemanning av driftssentral	23
7.10 Ekstern tilkobling til driftskontrollsystemet	24
7.11 Systemredundans i driftskontrollsystemet	26
7.12 (Opphevet)	28
7.13 Beskyttelse mot elektromagnetisk puls og interferens	28
7.14 Særskilte krav til driftskontrollsystemer i klasse 2	30
7.15 Særskilte krav til driftskontrollsystem klasse 3	38
7.16 Vern av kraftsystem i regional- og transmisjonsnett	42
7.17 Mobile radionett – driftsradio	44

7. Beskyttelse av driftskontrollsystem

Driftskontrollsystem er definert i § 7-1 i denne forskriften. I følge § 7-1 omfatter driftskontrollsystemer driftssentraler, utstyr, nettverk, datarom, sambandsanlegg og øvrige anlegg og rom, systemer og komponenter som ivaretar driftskontrollfunksjoner. Denne definisjonen er vid. Når enkelte krav er rettet mot det tekniske kontrollsystemet, er dette kommentert spesielt under hver paragraf.

Driftskontrollsystemer er avgjørende for situasjonsforståelsen, effektiv drift, håndtering av ekstraordinære situasjoner og rask og trygg gjenoppretting av feil og annen skade på system og infrastruktur. Driftskontrollsystemet må fungere og gi korrekt informasjon selv ved langvarige og ekstraordinære hendelser. Dersom driftskontrollsystemet svikter, må virksomheten ha beredskap og planer for alternativ drift.



Driftskontrollsystem og administrativt nettverk. Alt innenfor stiplede linje regnes som driftskontrollsystem (Kilde NVE Veiledning 2013).

Kapittel 7 setter krav til sikring av driftskontrollssystemet mot en rekke farer og trusler. §§ 7-14 og 7-15 i forskriften oppstiller tilleggskrav til virksomheter med driftskontrollsystemer i klasse 2 og 3.



Driftskontrollsystemer styrer tekniske anlegg i ulike klasser. I driftskontrollsystemer skal elektronisk/digital kommunikasjon og datautveksling sikres i henhold til driftskontrollsystemets klasse.

Driftssentral og datarom sikres fysisk i henhold til det fysiske anleggets klasse (se forskriftens kapittel 5 med vedlegg), eller driftskontrollsystemets klasse når denne er høyere enn det fysiske anleggets klasse.

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.

Ordforklaring

Driftssentral	Rom i bygning med driftskontrollsystem som ivaretar driftskontrollfunksjoner og består av skjerm, tastatur, server, datanettverk, UPC og annen nødstrøm, samt klimaanlegg. I tillegg inngår servere, rutere, UPC og annen nødstrøm, samt klimaanlegg i tilhørende datarom og sambandsrom.
Utsyr	Tekniske komponenter og instrumenter, herunder for eksempel dataskjermer, servere, tastatur, PLC, vern, brytere, svitsjer, rutere, sensorer mm og hjelpemateriell.
Komponent	Del av et system, instrumentdel
Samband	Se § 4-7

Bestemmelsen pålegger en generell plikt til å sikre driftskontrollsystemet. Bestemmelsen krever at driftskontrollsystemet skal virke og respondere som forventet på måleverdier og meldinger fra anlegg som overvåkes og på kommandoer gitt av operatører på driftssentralen eller lokalkontrollanlegget. Det er kun godkjente brukere som skal starte, endre eller stoppe kommandoer i systemet. Det er virksomheten som godkjenner brukere. Virksomheten skal beskytte driftskontrollsystemet mot alle typer uønskede hendelser, se § 2-3 som setter krav til risikovurdering. Hendelser som inngår i risikovurderingen, bør samsvare med hendelsene som legges til grunn for beskyttelsen av driftskontrollsystemet.

Sikkerhetsstyring og tilhørende dokumentasjon skal inngå som en del av virksomhetens internkontrollsystem (se § 2-10).

Det er kun KBO-enheter som får lov til å overvåke og styre nett- og produksjonsanlegg som er underlagt denne forskriften. Driftssentralssamarbeid mellom ulike KBO enheter er tillatt. Andre enn

KBO-enheter kan ikke overvåke nettet med bryterinnstillinger og utføre kobling. Det er tillatt at et vaktsselskap overvåker og beskytter et kraftforsyningsanlegg ved å ha vakter på stedet. Tilsvarende er det tillatt å benytte programvare for å overvåke og beskytte driftskontrollsystemet mot digitale trusler.

NVE skiller mellom fysisk og logisk sikring. Den fysiske sikringen av driftskontrollsystemet skal være tilpasset det stedet anlegget eller bygningen befinner seg, og skaden som kan skje dersom noen utfører for eksempel hærverk eller sabotasje på stedet. Den logiske sikringen skal være iht. den av de tilkoblede anleggene med høyest klassifisering. Anleggene skal beskyttes for påvirkning fra punkter på sambandsveien, samt skal beskyttes for påvirkning fra andre lokasjoner. Alle selskap må foreta en risikovurdering av sambandsstrukturen slik at driftskontrollsystemet ikke skal kunne påvirkes fra anlegg av lavere klassifisering, se også § 2-3 som setter krav til risikovurdering.

Fysisk sikring

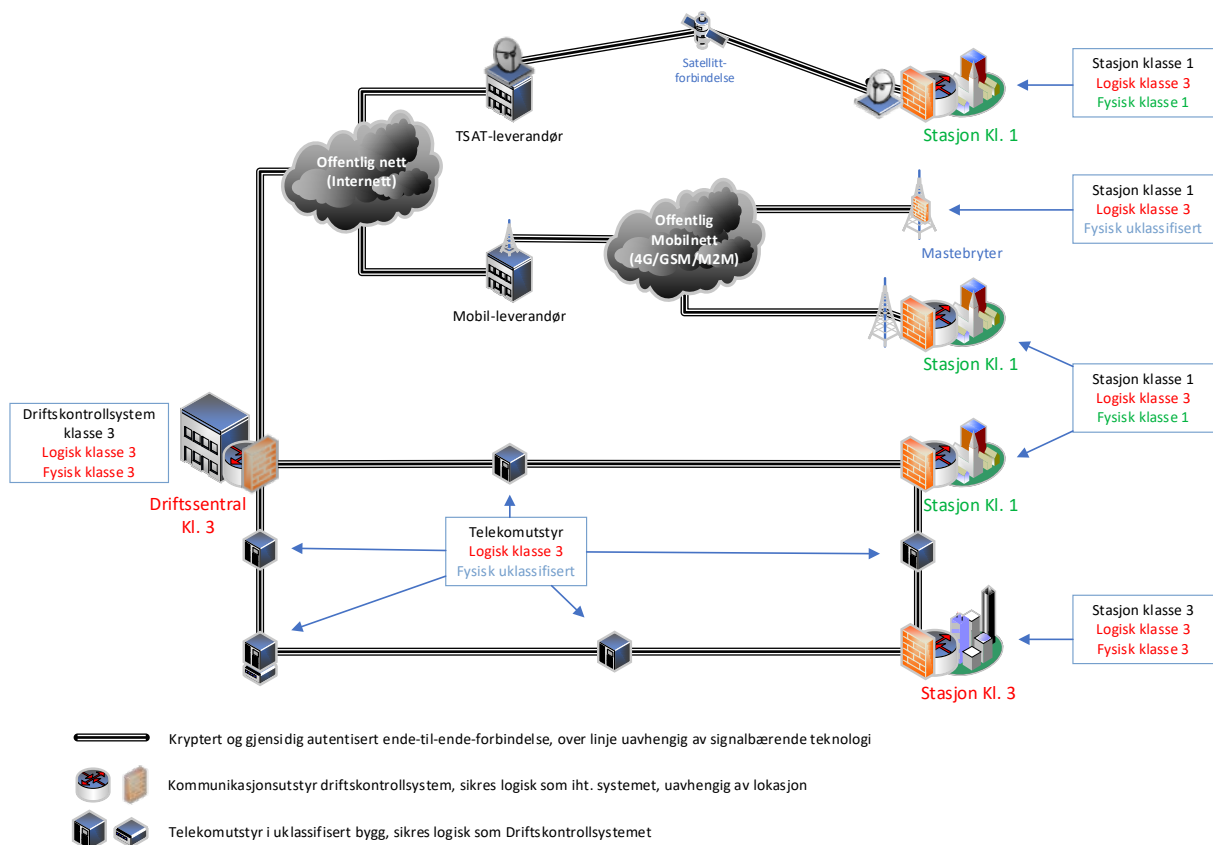
Sambandsanlegg og lokalkontrollanlegg går som regel gjennom skap via rekkeklemmer til avgrensning og fordeling, til forsterkere, antenner og annet. Slike skap er det ikke mulig å sikre etter driftskontrollsystemets klasse, og blir derfor sårbare angrepspunkt. I en klassifisert stasjon står skapene innenfor et gjerde eller inne i en bygning og er sikret med områdesikringen, skallsikringen eller sonesikringen. Utenfor klassifiserte anlegg har slike skap ingen sikring utover styrke og lås. Ved valg av skap, må vurderingen som er gjort angående skapets styrke, kvalitet på hengsler og lås, korrosjonsbeskyttelse og beskyttelse mot vann og fukt kunne dokumenteres.

Når signaler og målinger går i et redundant system, er ikke ødeleggelse av komponentene i et skap tilstrekkelig til å forhindre funksjonene i systemet. Uten redundans er ikke dette tilfelle. For sambandsanlegg viser vi til kravene i vedlegg 1, 2 og 3 til kapittel 5, punkt 1.2.2, 2.4.2 og 3.4.2.

Logisk sikring

Det skal alltid være ende-til-ende-kryptering i samband fra sentral til stasjoner, og mellom stasjoner, dersom kommunikasjon går over uklassifiserte eller lavere klassifiserte komponenter/linjer. Ende-til-ende-kryptering kan realiseres ved å sette ut utstyr foran driftsutstyret på stasjon/sentral eller ved direkte ende-til-ende-kryptering mellom SCADA og RTU. I tillegg må det iverksettes beskyttelsesmekanismer, som brannmur, portautentisering, osv. på driftssentral/stasjoner for å beskytte mot påvirkning fra en mulig kompromittert lokasjon. På denne måten vil en angriper ikke kunne få innsyn eller tilgang til andre komponenter dersom sambandet blir kompromittert, og vil ikke kunne bevege seg videre fra en stasjon som er kompromittert. Dette betyr at det verste som kan skje om noen tar seg inn til utstyret er at forbindelsen blir brutt. Dette vil man være beskyttet mot med redundante sambandsveier.

Denne type sikring skal gjelde uansett transmisjonsmedier, også om dette går via f.eks. mobilnett.



Standarder

[ISO/IEC 27019:2017 Information technology — Security techniques — Information security controls for the energy utility industry](#)

NEK 820: Cybersikkerhet for industrielle automatiserings- og kontrollsystemer er en samling av hele NEK EN IEC 62443-serien og gir en strukturert tilnærming for å utlede sikkerhetskrav for industriell automatisering og kontrollsystemer (IACS).

IEC 62443 Industrial Automation and Control Systems Security

NEK 850 A og B: Cybersikkerhet for kommunikasjonsprotokoller i elkraftsystemet er en samling av hele NEK EN IEC 62351-serien.

NERC-CIP (North American Electric Reliability Corporation critical infrastructure protection)

[NIST 800-82 Guide to Industrial Control Systems \(ICS\) Security](#)

Veiledere

[NSMs Grunnprinsipper for sikkerhetsstyring](#)

[Guide to Increased Security in Industrial Control Systems, MSB, Sverige](#)

[21 Steps to improve Cyber Security of SCADA networks, Department of Energy, USA](#)

[ICS Advisory \(ICSA-20-289-01\) Advantech WebAccess/SCADA, publisert 15.10.2020](#)
[Reducing cyber risks for industrial control systems \(ICS\), Professional Supplementary Document, Cyber Israel](#)

Krysskoplinger til annet regelverk

§ 5-1. Sikringsplikt

§ 5-2. Klasser

§ 6-9 Digitale informasjonssystemer

§ 6-10 Brytefunksjonalitet I avanserte måle- og styringssystem

[Forskrift om måling, avregning, fakturering av nettlestetjenester og elektrisk energi, nettselskapets nøytralitet mv](#) § 4-2 Funksjonskrav

7.2 Interne sikkerhetsregler

§

§ 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.

Virksomheter skal gjennomgå sikkerhetsreglene minimum årlig for å sikre at de etterleves og at de gir tilfredsstillende beskyttelse.

Hvordan oppfylle kravet

Virksomheter må omsette forskriftskravene til sikkerhetsregler som er tilpasset virksomheten. Sikkerhetsreglene må sørge for at virksomheten kan overvåke og kontrollere komponenter og anlegg i kraftforsyningen uten at dette arbeidet går på bekostning av sikkerheten. Virksomheten må også definere hva som er sikker drift av driftskontrollsystemet.

Sikkerhetsreglene er virksomhetens eget verktøy for å følge både kravene i forskriften og egne rutiner. Sikkerhetsreglene må være lett tilgjengelig der de skal brukes og bli gjort kjent for brukerne av reglene. Minst en gang i året skal virksomheten gjennomgå sikkerhetsreglene og vurdere behovet for å gjennomføre nødvendige endringer. I dette arbeidet kan det være hensiktsmessig å ta lærdom fra siste års arbeid og rette opp mangler man har erfart, se eksempel på sikkerhetsregler.



Eksempel: Sikkerhetsregler

Kraftkonsernet AS har utarbeidet et sett med sikkerhetsregler for følgende temaer i driftskontrollsystemet:

- ansvarsforhold og sikkerhetsinstruks for driftssentralen
- inndeling i sikkerhetssoner og segmentering av datanettverk
- tilgangsstyring – rollebasert tilgang logisk og fysisk samt passordregler
- hvitelisting av applikasjoner og tilganger – minimering av rettigheter
- styring og kontroll av lisenser
- minimering av eksponering av driftskontrollsystemet på internett
- tilgangsstyring og krav til rettmessige brukere, inklusive brukere hos leverandører
- testing, overvåkning og kontroll av sikkerhet
- sikkerhetskopiering og forsvarlig sletting av driftskritisk informasjon og kraftsensitiv informasjon
- håndtering av og sikring av bevis/dokumentasjon i uønskede hendelser, sikkerhetsbrudd og ekstraordinære situasjoner

Disse temaene er dokumentert, og dokumentene blir gjennomgått årlig for å vurdere relevans og gjennomføre forbedringer.



Standarder

§ 7-2 inneholder deler av mange standarder som et tiltak eller en kontroll:

- NS-EN ISO/IEC 27002:2017 Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring, se www.standard.no
- ISO/IEC 27002:2017 - Tiltak for informasjonssikring
 - o 5.1.1 Policies for information security
 - o 5.1.2 Review of the policies for information security
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.3.2.6 Security policies and procedures
- NIST 800-100 - Information Security Handbook: A Guide for Managers
 - o 2.2.5 Information Security Policy and Guidance
- NERC CIP-003-7 Security Management Controls
 - o R1 Cyber security policies

Veiledere

[Guide to Increased Security in Industrial Control Systems, MSB, Sverige](#)

[21 Steps to improve Cyber Security of SCADA networks, Department of Energy, USA](#)

[Reducing cyber risks for industrial control systems \(ICS\), Professional Supplementary Document, Cyber Israel](#)

Krysskoplinger til annet regelverk

§ 2-10 Internkontroll

§ 5-1. Sikringsplikt

§ 5-2. Klasser

§§ 5-3, 5-4, 5-5 og 5-6 Sikringstiltak for klassifiserte anlegg avhengig av klasse

§ 6-9 Digitale informasjonssystemer

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

§7-14b. Sikkerhetsrevisjon - for klasse 2 og klasse 3 driftskontrollsystem

[Forskrift om måling, avregning, fakturering av netttjenester og elektrisk energi, nettselskapets nøytralitet mv](#) § 4-2 Funksjonskrav og § 4-6 krav til sikkerhet for AMS

7.3 Dokumentasjon av driftskontrollsystemet

§

§ 7-3. Dokumentasjon av driftskontrollsystemet

Virksomheter skal til enhver tid ha oppdatert dokumentasjon av driftskontrollsystemet.

I dokumentasjonen skal det inngå en oversikt over alle sikkerhetstiltak som er implementert. Dokumentasjonen skal også omfatte en oppdatert skjematisk fremstilling av driftskontrollsystemets logiske og fysiske nettverk som viser eventuelle tilgangspunkt mellom driftskontrollsystemet og andre nettverk. Dokumentasjonen skal også omfatte en komplett oversikt over utstyr i driftskontrollsystemet.

Ordforklaring

Dokumentasjon	Tegning, bilde eller tekst lagret og gjenfinnbart på digitale medier eller på papir
Logisk nettverk	Logiske nettverk består av: Datanettverk, inkludert IP-adresser, VLAN, subnett, DMZ.
Fysisk nettverk	Geografiske føringer av datakabler, radiolinker, plasseringer av brannmur, rutere, svitsjer, PLS-er, RTU-er, servere.
Utstyr	Tekniske komponenter og instrumenter, herunder for eksempel dataskjermer, servere, tastatur, PLC, vern, svitsjer, rutere, sensorer mm.
Implementert	Installert og tatt i bruk

Hvordan oppfylle kravet

Dokumentasjonen skal være oppdatert, tilstrekkelig detaljert og relevant slik at brukere av dokumentasjonen ikke er i tvil om egenskaper, konfigurasjon eller innstillinger til datanettverket som benyttes i prosessstyring eller driftskontroll. Dokumentasjonen må sette aktuelle brukere av dokumentasjonen i stand til å gjenopprette driftskontrollsystemet etter feil, svikt eller innbrudd i systemet. Dokumentasjonen skal være tilgjengelig også uten internettforbindelse, se § 6-8. Dette gjelder både internt og ved fjernlagring.

Den skjematiske fremstillingen skal dekke både det logiske og det fysiske datanettverket. Det skal tydelig komme fram der driftskontrollsystemet er koblet til andre datanettverk som for eksempel administrasjonsnett, leverandør, AMS og Elcom/Inter Control Center Communication Protocol (ICCP).

Formen på dokumentasjonen bør være på et format som fungerer godt for formålet – å kunne drifte og gjenopprette i normal og i ekstraordinære situasjoner. For noen er dette regneark, for andre er det egne systemer, GIS eller tegninger.



Eksempel: Hvordan strukturere dokumentasjon for driftskontrollsystem

Kraftkonsernet AS har følgende dokumentasjon:

- Oversikt over fysiske komponenter (eksempelvis rutere, servere, målere mm.)
 - Produktdokumentasjon fra leverandører av de ulike komponentene i driftskontrollsystemet
- Konfigurasjonsfiler til komponenter, eks. brannmur, IDS, vern
 - Programvare med versjonsnummer
 - Standardinnstillinger og beskrivelse av virksomhetens egne konfigurasjoner av de ulike komponentene
- Systemarkitektur, se Open Systems Interconnection model (OSI model) for lagdeling av digitale systemer
 - Logisk datanettverk med soneinndeling og sikringstiltak, eks. brannmur, innbruddsdeteksjonssystemer (IDS) mv.
 - Fysisk datanettverk
- Beskrivelse av hvordan man fysisk har sikret de ulike komponentene i driftskontrollsystemet

Kraftkonsernet AS har en skriftlig prosedyre for å dokumentere endringer i systemet og en revisjonslogg for dokumentet.



Standarder

§ 7-3 inneholder deler av mange standarder og veiledere som et tiltak eller en kontroll:

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyning
 - o 8.1.1 Inventory of assets
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.2.3.4 Identify the IACS
 - o 4.2.3.5 Develop simple network diagrams
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - o 4.5.1 Categorize ICS Systems and Networks Assets
- NERC CIP-002-5.1a BES Cyber System Categorization
 - o R1 Identification and documentation of assets

Veileder

NSMs Grunnprinsipper for IKT-sikkerhet – Identifisere og dokumentere

Krysskoplinger til annet regelverk

§ 2-10 Internkontrollsystem

§ 6-2 a Kraftsensitiv informasjon

§ 6-3 Beskyttelse, avskjerming og tilgangskontroll

§ 6-8 Sikkerhetskopier

§ 6-9 a. Digitale informasjonssystemer



Eksempel: Registrering av komponenter

For å kunne ha en sikker drift og tilstrekkelig oversikt over driftskontrollsystemet, må dokumentasjonen oppdateres hver gang det kommer nye komponenter inn i systemet eller det gjennomføres en oppgradering av programvare. Dersom IKT-sikkerhetskoordinator ikke vet hvilken versjon av programvaren som ligger på komponentene, kan han heller ikke vurdere sårbarhetsvarsler han får fra KraftCERT (se § 3-6) og lukke sårbarhetene. Dersom han ikke har oversikt over de tekniske egenskapene til de enkelte enhetene, vet han heller ikke om det er skjulte veier inn i systemet, for eksempel en mobilsender/mottaker som ikke er skrudd av eller et standardpassord som ikke er endret.

IKT-sikkerhetskoordinator vurderer samtidig kravene til sikkerhetskopier av denne dokumentasjonen.



Digitale systemer trenger å bli oppdatert og feilrettet. Ta kontakt med KraftCERT dersom det er leverandører som ikke varsler om sårbarheter. Da kan KraftCERT følge opp leverandøren. Se §§ 3-6 og 6-9.

7.4 Kontroll med brukertilgang



§ 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.

Virksomheter skal kontrollere hvilken bruker som er eller har vært pålogget driftskontrollsystemet, også når ekstern tilkobling brukes.

Kontrollordningene skal gjennomgås minimum årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå.

Ordforklaring

Rettmessig bruker	Person eller applikasjon som er godkjent av virksomheten for tilgang
Tilgangsrettighet	En brukers rett til å skrive, endre og lese data
Tilgang	Logisk og fysisk tilgang
Kontrollordning	Fremgangsmåte eller tiltak for å sørge for kontroll

Hvordan oppfylle kravet

Virksomheten må ha en prosedyre for å godkjenne og slette brukere (klarere brukere og autorisere tilgang og rettigheter). Virksomheten må til enhver tid ha oversikt over hvem som har tilgang til driftskontrollsystemet og hvilke handlinger de har lov til å utføre. Virksomheten må også ha en oversikt over - og kunne registrere og kontrollere - hvilke brukere som har vært pålogget eller aktive i driftskontrollsystemet til et hvilket som helst tidspunkt.

Virksomheten må sørge for at brukere ikke har flere rettigheter i domenet til driftskontrollsystemet enn nødvendig. Et minimum av brukere skal ha administratorrettigheter. Å benytte en sentralt styrt brukeradministreringsløsning med rettighetshåndtering, for eksempel Active Directory, vil lette kontrollen med brukerrettigheter i domenet til driftskontrollsystemet.

Eksterne leverandører får ikke lov til å på egenhånd, og uten kontroll fra virksomheten, administrere beskyttelsestiltakene for driftskontrollsystemet. De skal for eksempel ikke oppdatere regelsett for brannmurer eller konfigurere nettverkssvitsjer uten virksomhetens godkjenning og overvåkning. Sesjoner og endringer skal logges og kunne revideres.

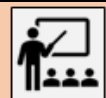
Minst en gang i året skal de forskjellige prosedyrene og kontrollordningene for tilgangsrettigheter gjennomgås. Målsettingen er å sikre at tilgangsrettighetene fortsatt er riktige og prosedyrene relevante. I gjennomgangen skal man også kontrollere at eventuelle endringer og/eller slettinger av tilgang har blitt gjennomført. Merk at tilgangskontroll også inkluderer sikker oppkobling mot driftskontrollsystemet og passordpolitikk. Virksomheten skal også ha kontroll med fysisk tilgang til driftskontrollsystemet, jf. den brede definisjonen av driftskontrollsystemet i § 7-1, og kunne revidere hvem som har hatt tilgang.



NSMs anbefaling for virksomheter

- Innfør to-faktor autentisering
- Unngå at passord lagres i klartekst
- Innfør rutiner for å kontrollere nye passord mot mye brukte og kompromitterte passord
- Innfør rutiner for å bytte standardpassord på nytt utstyr
- Gi brukere som trenger administratorrettigheter to kontoer

Det finnes også tjenester som <https://haveibeenpwned.com/> der domeneiere og IT-administratorer kan få varsler dersom en epost-adresse i domenet dukker opp i en lekkasje.



Eksempel: Tilgang til driftskontrollsystemet

Nett AS blir revidert av NVE. Revisorene stiller spørsmål om tilgangskontrollen til driftskontrollsystemet. IKT-sikkerhetskoordinatoren forklarer at ansatte på driftssentralen har gruppetilgang med felles påloggingsinformasjon. NVEs revisor påpeker at dette ikke er godt nok, det skal være personlige brukere. Om dette ikke er mulig, skal brukeres tilgang og tilstedeværelse registreres i et annet system eller manuelt. Hvem som har hatt tilgang skal være mulig å spore. NVE anbefaler separat Active Directory for driftskontrollsystemet når det er mulig og å følge NSMs passordråd.



Standarder

§ 7-4 inneholder deler av mange standarder som et tiltak eller en kontroll:

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyning
 - o 9.1.1 Access control policy
 - o 9.1.2 Access to networks and network services
 - o 9.2.1 User registration and de-registration
 - o 9.2.2 User access provisioning
 - o 9.2.3 Management of privileged access rights
 - o 9.2.4 Management of secret authentication information of users
 - o 9.2.5 Review of user access rights
 - o 9.2.6 Removal or adjustment of access rights
 - o 9.3.1 Use of secret authentication information
 - o 9.4.1 Information access restriction
 - o 9.4.2 Secure log-on procedures
 - o 9.4.3 Password management systems
 - o 9.4.4 Use of privileged utility programs
 - o 9.4.5 Access control to program source code
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.3.2.6 Security policies and procedures
 - o 4.3.3.5 Access control – Account administration
 - o 4.3.3.6 Access control – Authentication
 - o 4.3.3.7 Access control – Authorization
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - o 6.2.1 Access control
- NERC CIP-004-6 Personnel and training
 - o R4 Access Control
- NERC CIP-007-6 System Security Management
 - o R5 System Access Control

Veiledere

NSM Grunnprinsipper for IKT-sikkerhet

- o 1.3 Kartlegg brukere og behov for tilgang
- o 2.6 Ha kontroll på identiteter og tilganger

[NSM Råd og anbefalinger om passord](#)

Krysskoplinger til annet regelverk

§ 5-11 Restriksjoner for adgang til steder og områder

§ 7-10 Ekstern tilkobling til driftskontrollsystemet

§ 7-14 f Ekstern tilkobling til driftskontrollsystemet for klasse 2 og 3 og § 7-15 c

Overvåking og logging for klasse 3 driftskontrollsystem

§ 7-14c. Overvåkning og logging for klasse 2 og klasse 3 driftskontrollsystem.

§ 6-9 Digitale informasjonssystemer

7.5 Kontroll ved endringer i driftskontrollsystemet



§ 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.

Hvordan oppfylle kravet

Virksomheten må ha forebyggende sikringstiltak og prosedyrer i internkontrollsystemet (ref § 2-10) som beskriver hvordan virksomheten vurderer, tester og godkjenner endringer i driftskontrollsystemet enten det er fysiske endringer eller endringer i programvare. Endring kan inkludere oppdateringer av programvare, konfigurasjonsendringer, oppgradering og utskifting av system eller komponenter. Prosedyrene og tiltakene må legges til grunn for avtalen med leverandører som driver vedlikehold på driftskontrollsystemet.

For å hindre utilsiktede feil og nye sårbarheter, må det utføres tester av at endringen er trygg og at systemet fungerer etter hensikten også etter at endringen er utført.

Før større endringer, for eksempel oppgradering til ny versjon, må virksomheten kartlegge mulige negative konsekvenser som endringen kan medføre. Ved store endringer må det også foreligge en plan for å håndtere uforutsette hendelser som skjer under endringsprosessen.

Virksomheten bør fastsette egne kriterier for hvilke endringer som krever en egen risikovurdering før endringene gjennomføres.



Eksempel: Endringer i driftskontrollsystemet etter varsel fra KraftCERT

IKT-sikkerhetskoordinator har mottatt sårbarhetsvarsel fra KraftCERT på en komponent virksomheten har i sitt driftskontrollsystem. KraftCERT skriver i sitt varsel at dette er en kritisk sårbarhet der en mulig angriper kan skaffe seg administrator-rettigheter.

KraftCERT anbefaler selskapene å oppdatere programvaren og ta kontakt med leverandøren for mer informasjon.

IKT-sikkerhetskoordinator forstår at det er viktig å redusere en så alvorlig sårbarhet i driftskontrollsystemet. SCADA-systemet er duplisert, og oppdateringen utføres av leverandøren og testes først på det ene systemet, før det andre systemet blir oppdatert.



Maler

Melding om klassifisering av driftskontrollsystem

Standarder

§ 7-5 inneholder deler av mange standarder og veiledere som et tiltak eller en kontroll:

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
 - o 12.1.2 Change management
 - o 12.1.4 Separation of development, testing and operational environments
 - o 14.2.1 Secure development policy
 - o 14.2.2 System change control procedures
 - o 14.2.3 Technical review of applications after operating platform changes
 - o 14.2.4 Restrictions on changes to software packages
 - o 14.2.8 System security testing
 - o 14.2.9 System acceptance testing
 - o 14.2.10 ENR – Least functionality
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.3.2.6 Security policies and procedures
 - o 4.3.4.3 System development and maintenance
- IEC 62443-2-3 – Patch management for the IACS environment
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - o 6.2.5 Configuration Management
- NERC CIP-007-6 System Security Management
 - o R2 Security patch management
- NERC CIP-010-2 Configuration Change Management and Vulnerability Assessments
 - o R1 Configuration Change Management

Veileder

- NSM Grunnprinsipper for IKT-sikkerhet
 - o 2.10 Integrer sikkerhet i prosess for endringshåndtering

Krysskoplinger til annet regelverk

§ 6-9 b. Risikovurdering

§ 7-10 Ekstern tilkopling til driftskontrollsystemet

§ 7-14 f. Ekstern tilkobling til driftskontrollsystemet for klasse 2 og klasse 3 driftskontrollsystem,

7-15c Ekstern tilkobling til driftskontrollsystemet for klasse 3 driftskontrollsystem

7.6 Kontroll med utstyr i driftskontrollsystemet



§ 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.

Virksomheter skal hindre urettmessig tilgang mellom driftskontrollsystemet og andre informasjonssystemer.

Virksomheter skal hindre urettmessig tilgang til utstyr som benyttes for å etablere logiske eller fysiske skiller mellom driftskontrollsystemet og andre informasjonssystemer.

Virksomheter skal permanent slette all informasjon i utstyr som ikke lenger skal brukes i driftskontrollsystemet.

Det er ikke tillatt å bruke personlig eid utstyr i driftskontrollsystemet.

Datakommunikasjon i driftssentral og datarom skal være trådbundet.

Beredskapsmyndigheten kan i særskilte tilfeller forby bruk av enkelte typer utstyr.

Ordforklaring

Logiske skiller	Programvare som inspiserer og stopper ikke godkjent datatrafikk i henhold til forhåndsdefinerte kriterier
Fysiske skiller	Maskinvare, elektroniske komponenter og dørlås, sperringer som begrenser tilgang i henhold til virksomhetens sikkerhetsregler
Trådbundet	Kablet

Hvordan oppfylle kravet

Utstyr som benyttes i driftskontrollsystemet, skal kun benyttes der. Utstyret skal aldri brukes midlertidig i andre nettverk eller til andre oppgaver eller formål. En PC knyttet til administrasjonsnettverket eller som er brukt til et annet formål, kan ikke senere benyttes i driftskontrollsystemet. En PC brukt i driftskontrollsystemet kan ikke brukes til noe annet etterpå. Den kan gjenbrukes dersom data er permanent slettet eller lagringsmediene er destruert.

Virksomheten skal sikre at det kun er rettmessige applikasjoner, IP-adresser, maskinvare og personer som har tilgang til driftskontrollsystemet. Utgangspunktet er ingen tilgang, og tilgang gis kun etter godkjenning fra virksomheten (hvitlisting).

Virksomheten skal sørge for at det kun er godkjente brukere som har tilgang til for eksempel brannmur, innbruddsdeteksjon, klienter, svitsjer, låsesystemer etc. Godkjente brukere kan være egne ansatte eller leverandører som drifter systemet eller tjenesten på vegne av, og under kontroll av, virksomheten. Det er virksomheten som bestemmer hvilken tilgang og hvilke rettigheter de godkjente brukerne skal ha.

Når utstyr eller komponenter ikke lenger skal benyttes i driftskontrollsystemet og heller ikke mellomlagres på sikkert sted som sikkerhetskopi eller reserve, skal informasjonen slettes permanent slik at den ikke kan gjenskapes. Utstyret skal heller ikke gjenbrukes og må derfor destrueres.

Bestemmelsen presiserer at privat utstyr ikke er tillatt å bruke i driftskontrollsystemet. Personlig eid utstyr er ikke omfattet av virksomhetenes sikkerhets- og kontrollregime og kan derfor være mer mottakelig for skadelig programvare og feil.

Med trådløse nettverk menes for eksempel bruk av trådløse rutere (wifi) eller blåtann (Bluetooth) for å overføre nettverkstrafikk basert på bruk av lokale radiosignaler. Trådløs overføring av data er ikke tillatt fordi trådløs kommunikasjon er sårbar for blokkering (interferens mv). På driftssentralen og i datarommet (serverrommet) skal derfor kabler kople sammen servere og klienter, datamus og tastatur.

Bestemmelsen regulerer ikke bruk av radiolinje eller satellittkommunikasjon som samband for overføring av styringssignaler i driftskontrollsystemet.



Eksempel: Kontroll med utstyr som koples til driftskontrollsystemet

IKT-sikkerhetskoordinator mener et viktig tiltak for å sørge for at utstyr kun blir brukt i driftskontrollsystemet, er å etablere en rutine som beskriver hvordan kravet skal etterleves og sørge for at rutinen faktisk blir fulgt.

Det er ikke tillatt å benytte privat nettbrett, PC, telefon, mus, lader og minnepinner i driftskontrollsystemet. Dette kravet skrives inn i interne sikkerhetsregler rettet mot ansatte, leverandører og innleide, og dokumenteres i internkontrollsystemet.

IKT-sikkerhetskoordinator tar videre utgangspunkt i oversikten han har over alt utstyr i driftskontrollsystemet. Alt utstyr som brukes i driftskontrollsystemet er merket slik at det er enkelt å kjenne igjen for dem som skal bruke det. Utstyret skal videre konfigureres slik at det kun er godkjente komponenter som får bli koplet til driftskontrollsystemet. Rutine for oppdatering av utstyrsoversikter finnes i internkontrollsystemet.

Når rutinen er etablert, er det viktig å sørge for at rutinen blir fulgt, ellers har den ingen effekt.



Standarder

§ 7-6 inneholder deler av mange standarder og veiledere som et tiltak eller en kontroll:

- ISO/IEC 270019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen (ikke uttømmende liste)
 - o 8.1.1 Inventory of assets
 - o 8.1.2 Ownership of assets
 - o 8.1.3 Acceptable use of assets
 - o 8.1.4 Return of assets
 - o 8.2.3 Handling of assets
 - o 8.3.1 Management of removable media
 - o 8.3.2 Disposal of media
 - o 8.3.3 Physical media transfer
 - o 11.2.1 Equipment siting and protection
 - o 11.2.3 Cabling security
 - o 11.2.5 Removal of assets
 - o 11.2.6 Security of equipment and assets off-premises
 - o 11.2.7 Secure disposal or re-use of equipment
 - o 11.2.8 Unattended user equipment
 - o 11.3.1 ENR – Equipment sited on the premises of other energy utility organizations
 - o 11.3.2 ENR – Equipment sited on customer's premises
 - o 11.3.3 ENR – Interconnected control and communication systems
 - o 12.8.1 ENR – Treatment of legacy systems
 - o 13.1.3 Segregation of networks
 - o 13.2.1 Information transfer policies and procedures
 - o 14.2.10 ENR – Least functionality
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.3.2.6 Security policies and procedures
 - o 4.3.3.4 Network segmentation
 - o 4.3.4.3 System development and maintenance
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - o 4.5.1 Categorize ICS Systems and Networks Assets
- NERC CIP-002-5.1a BES Cyber System Categorization
 - o R1 Identification and documentation of assets

Veiledere

- NSM sine grunnprinsipper for IKT-sikkerhet
 - o 1.2 Kartlegg enheter og programvare
- Nettvett – Metoder for sikker sletting av informasjon,
<https://nettvett.no/sikker-sletting/>

Krysskoplinger til annet regelverk

§ 7-3 Dokumentasjon av driftskontrollsystemet

§ 2-10 Internkontrollsystem

7.7 Håndtering av feil, sårbarheter og sikkerhetsbrudd



§ 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.

Virksomheter skal ha tilgang til tilstrekkelig personell med nødvendig kompetanse som uten unødig opphold kan håndtere forhold angitt i første ledd.

Virksomheter skal registrere alle sikkerhetsbrudd og -hendelser.

Forhold som kan utgjøre en umiddelbar risiko for driftskontrollsystemets funksjon, skal varsles og rapporteres til beredskapsmyndigheten, jf. § 2-5 og § 2-6.

Hvordan oppfylle kravet

Virksomheten må kunne rette feil, oppdatere programvare, håndtere sikkerhetsbrudd og andre uønskede hendelser slik at virksomheten evner å opprettholde funksjonaliteten til driftskontrollsystemet. For å ha oversikt over sårbarheter, anbefaler NVE virksomhetene å følge med på sårbarhetsvarsler og sikkerhetsråd utsendt fra KraftCERT og fra virksomhetens leverandører.



KraftCERT samler informasjon om aktuelle sårbarheter og trusler fra en rekke kilder og videreformidler informasjon og kritiske sårbarheter til virksomheter i kraftbransjen. Virksomheten bør sørge for at IKT-sikkerhetskoordinator eller en annen ansatt abonnerer og følger med på råd fra KraftCERT.

Virksomheten må ha system, programvare og utstyr på plass som bistår med teknisk overvåkning av datanettverk og komponenter, oppdagelse av og varsling av feil og uønskede hendelser. Virksomheten må også ha prosedyre for hendelseshåndtering og feilretting der ansvar og aksjonspunkter framgår. Interne prosedyrer må samkjøres med ekstern leverandørs prosedyrer i supportsituasjoner der det er aktuelt. Merk at avtale om support i helligdager og utenom arbeidstid må inngå i avtalen med leverandøren.

NVE anbefaler at virksomhetene har tilgang til et sikkerhetsoperasjonssenter (SoC), enten eget eller som kjøpt tjeneste. SoC kan overvåke varsler og feilsituasjoner, samt bidra med hendelseshåndtering. KraftCERT kan gi råd i forbindelse med anskaffelse av slik tjeneste. NSM har en godkjenningsordning for leverandører av sikkerhetstjenester.

Virksomheten må ha tilgang til eget personell med relevant kompetanse eller ha tilgang til kompetent personell gjennom innleie eller avtale med leverandør. Det kreves ulik kompetanse for å kunne håndtere feil i nett og anlegg kontra det å håndtere IKT-sikkerhetsbrudd. NVE anbefaler virksomhetene å bygge egen tverrfaglig kompetanse på elkraft, operasjonell teknologi (OT) og IKT-

sikkerhet. Virksomheten må uansett ha tilstrekkelig kompetanse til å kunne utforme kravspesifikasjon og følge opp leverandør hvis oppgavene settes ut.

Informasjon om egne sikkerhetsbrudd, herunder logger, må registreres og lagres trygt, beskyttet og med minimal risiko for uautorisert endring, jf. kapittel 6. I noen tilfeller vil sikkerhetsbrudd- og hendelser bli automatisk registrert i flere forskjellige systemer. Hvis ikke informasjon samles i et felles system, må virksomheten ha et dokument som beskriver hvor logininformasjon finnes. Dersom virksomheten opplever sikkerhetsbrudd eller blir utsatt for en kriminell handling, kan tidsseriedata være viktige for etterforskningen. Logger bør lagres minimum to år av hensyn til mulig etterforskning.

Virksomheten skal varsle NVE dersom det skjer hendelser i driftskontrollsystemet som kan utgjøre en fare for dets funksjon. Det skal foreligge en rutine for slik varsling. Det kan for eksempel være systemfeil som fører til tap av overvåking og kontroll, ikke godkjent tilgang til eller endring av systemet som følge av datainnbrudd. Varsel skal sendes uten ugrunnet opphold jf. § 2-5. Rapport skal sendes etter at hendelsen er håndtert, jf. § 2-6.

I tillegg følger det av § 6-9 c at virksomheten skal varsle uønskede hendelser i sine digitale informasjonssystemer til den beredskapsmyndigheten bestemmer. NVE peker på KraftCERT. KBO-enhetene må varsle KraftCERT om alle uønskede IKT-hendelser. Dette er en praktisk ordning for KBO og NVE. Deling av opplysninger om hendelser og suspekt aktivitet med KraftCERT vil være til nytte for etablering av et mer detaljert og relevant situasjonsbilde i kraftforsyningen. Gjennom høy delaktighet og lav terskel for å dele, vil den kollektive situasjonsforståelsen og evnen til læring og beskyttelse blir bedre. § 2-5 og § 2-6 gir bestemmelser om hendelser som skal varsles og rapporteres til NVE. Merk at kraftsensitiv informasjon må beskyttes som angitt i kapittel 6.



Standarder

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
 - o 16.1.1 Incident management – Responsibilities and procedures
 - o 16.1.2 Reporting information security events
 - o 16.1.3 Reporting information security weaknesses
 - o 16.1.4 Assessment of and decisions on information security events
 - o 16.1.5 Response to information security incidents
 - o 16.1.6 Learning from information security incidents
 - o 16.1.7 Collection of evidence
 - o 12.2.1 Controls against malware
 - o 12.4.1 Event logging
 - o 12.6.1 Management of technical vulnerabilities
 - o 17.1.1 Planning information security continuity
 - o 17.1.2 Implementing information security continuity
 - o 17.1.3 Verify, review and evaluate information security continuity
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.3.2.6 Security policies and procedures
 - o 4.3.4.3 System development and maintenance
 - o 4.3.4.5 Incident planning and response
- IEC 62443-2-3 – Patch management for the IACS environment

- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - o 6.2.6 Contingency planning
 - o 6.2.8 Incident response
- NERC CIP-008-5 Incident reporting and response planning
 - o R1, R2, R3 Cyber security incident response plan
- NERC CIP-009-6 Recovery Plans for BES Cyber systems
 - o R1, R2, R3 Recovery plan

Veiledere

- NSM sine grunnprinsipper for IKT-sikkerhet
 - o 3.2 Etabler sikkerhetsovervåkning
 - o 4 Håndtere og gjenopprette
- [Logging og logganalyse i energiforsyningen. Studentrapport. NVE-rapport 1:2017](#)
- [Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem. Rapport utarbeidet av BDO AS for Norges vassdrags og energidirektorat, NVE-rapport 14:2017](#)

Krysskoplinger til annet regelverk

§ 2-4 Beredskapsplanlegging
 § 2-5 Varsling
 § 2-6 Rapportering
 § 4-1 Reparasjonsberedskap
 § 4-2 Kompetanse og personell
 § 4-4 Materiell og utstyr
 § 6-9 Digitale informasjonssystemer
 § 7-14 c Overvåkning og logging – for klasse 2 og 3 driftskontrollsystem

7.8 Beredskap ved svikt i driftskontrollsystemet

§

§ 7-8. Beredskap ved svikt i driftskontrollsystemet

Virksomheter skal ha beredskap og forberedte tiltak for fortsatt drift av anlegg ved svikt i driftskontrollsystemet.

Hvordan oppfylle kravet

Bestemmelsen stiller krav til at virksomheten skal ha forberedt nødvendige tiltak for å drifte sine anlegg selv om driftskontrollsystemet er degradert eller slutter å virke. Virksomheten må derfor ha en beredskapsplan som beskriver hvordan driften av anleggene skal gjøres i en slik situasjon og ikke minst hvordan virksomheten skal få gjenopprettet systemet igjen. I dette inngår å reetablere ved å benytte sikkerhetskopier og installere systemet på nytt dersom det er behov for det.

Planen bør inneholde en beskrivelse av hvordan anleggene skal driftes dersom driftskontrollsystemet blir utilgjengelig over lengre tid (dager, uker). Den bør beskrive ansvar, kontaktinformasjon og plan

for bemanning av anleggene over tid slik at anleggene kan styres manuelt ved behov. Se også vedlegg 2 og 3 i forskriften (pkt. 2.1.4 og 3.1.4). Beredskapsplanen bør også inkludere prosedyrer for driftskommunikasjon og kommunikasjon med virksomhetens ledelse dersom lokal bemanning og manuell styring er nødvendig. Beredskapsplanen bør også henvise til hvor man finner nødvendig systeminformasjon, eventuelt papirkopier av kritisk informasjon.

Manuell styring krever kompetanse som ikke blir brukt til daglig. Manuell styring av anlegg må derfor være forberedt og inngå som en del av øvelsesplanen til selskapet etter §§ 2-7 jf. også 7-14 d. NVE anbefaler å øve med et representativt anlegg, og om mulig rullere på anlegg og personell, og ha ulike scenarier.



Standarder

- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - 4.3.4.5 Incident planning and response
- IEC 62443-2-3 – Patch management for the IACS environment
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - 6.2.6 Contingency planning
 - 6.2.8 Incident response
- NERC CIP-008-5 Incident reporting and response planning
 - R1, R2, R3 Cyber security incident response plan
- NERC CIP-009-6 Recovery Plans for BES Cyber systems
 - R1, R2, R3 Recovery plan

Veiledere

- NSM Grunnprinsipper for IKT-sikkerhet
 - Håndtere og gjenopprette

Krysskoplinger til annet regelverk

§ 2-4 Beredskapsplanlegging

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

§ 7-14 d. Utløst driftssentral - klasse 2 og 3 driftskontrollsystem

7.9 Bemanning av driftssentral



§ 7-9. Bemanning av driftssentral

Virksomheter skal til enhver tid ha tilstrekkelig og tilgjengelig autorisert personell med nødvendig kompetanse, slik at driftskontrollfunksjonen kan utøves uten ugrunnet opphold.

Virksomhetens risikovurdering skal ligge til grunn for valg av bemanningens størrelse samt omfang av ordninger for påkalling av ekstra personell ved behov, jf. §§ 2-4 og 5-8.

Ordforklaring

Autorisert	Godkjent av virksomheten – funnet kvalifisert og sikkerhetsmessig egnet og har tjenestemessig behov
-------------------	---

Hvordan oppfylle kravet

Virksomheten skal gjøre en vurdering av hva som er nødvendig kompetanse for å utføre jobben og autorisere personell som har kvalifikasjoner og er sikkerhetsmessig egnet. Virksomheten må også ha en prosedyre for å godkjenne personell som skal arbeide som operatør i driftssentralen og gi nyansatte og fast ansatte ved driftssentralen tilstrekkelig opplæring og trening. Læring skjer gjennom daglig arbeid, kurs og øvelser.

Virksomheten skal ha en prosedyre for å vurdere i hvilken grad bemanningen er tilstrekkelig for å betjene driftssentralen, og i hvilken grad påkallingsordningens omfang er tilstrekkelig. Til grunn for vurderingene skal virksomheten gjøre en risikovurdering. Dette er et grunnleggende krav for alle KBO-enheter med driftskontrollsystemer eller virksomheter med driftskontrollsystemer der NVE har fattet vedtak om at virksomheten underlegges kravet. Det er tilleggskrav for driftskontrollsystemer i klasse 2 og 3, se §§ 7.14 d og e, og -7-15 b.



Kompetanse for personell som utøver driftskontrollfunksjoner

- Fagkunnskap om tekniske anlegg og om driftskontrollsystemet
- Oversikt over forsyningsområdet
- Inngående kjennskap til virksomhetens beredskapsplanverk og prosedyrer for håndtering av kompliserte feilsituasjoner
- Kompetanse i krisehåndtering (kan opparbeides gjennom øvelser)
- Språkkunnskaper i norsk og engelsk



Veiledere

- [NSR, Politiet, NSM, "Sikkerhet ved ansettelsesforholdNSR", og andre veiledere fra NSRs nettside](#)
- [NSM Temarapport Innsiderisiko.](#)

Krysskoplinger til annet regelverk

§ 2-4 Beredskapsplanlegging

§ 2-10 Internkontroll

§ 4-2 Kompetanse og personell

§ 7-14 e Bemanning av driftssentral

§ 7-15 b Bemanning av driftssentral

§ 5-8 Vurdering

§ 6-7 Personkontroll

Det er tilleggskrav for driftskontrollsystemer i klasse 2 og 3, se §§ 7.14 d.

Utilgjengelig driftssentral, e Bemanning av driftssentral, og 7-15 b Systemredundans.

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 avvike 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.

Hvordan oppfylle kravet

Tilkobling til et driftskontrollsystem fra en applikasjon, tjeneste eller maskin, fra bruker på hjemmekontor eller fra en bruker hos en leverandør i dennes lokaler, er en ekstern tilkobling. Ekstern tilgang skal normalt være stengt og kun åpnes når det er behov. Med tilgang menes her logisk tilgang.

Virksomheten kan oppfylle kravet om å ha kontroll ved å sørge for at tilgang til driftskontrollsystemet må godkjennes på forhånd av personell som virksomheten har bemyndiget. Virksomheten må ha prosedyrer for å godkjenne brukere, administrere logisk tilgang og brukerrettigheter.

Virksomheten må ha en prosedyre som beskriver forløpet fra operatør på driftssentralen gir tilgang til ekstern tilkobling og til den eksterne tilkoblingen er lukket.

Det skal til enhver tid være en oppdatert liste over brukere (personer, applikasjoner og maskinvare) som virksomheten har gitt tillatelse til å koble seg på driftskontrollsystemet.

Virksomheten må ha prosedyre i kombinasjon med tekniske tiltak og personelltiltak for å godkjenne, vedlikeholde og avvike tilgang til driftskontrollsystemet. Tekniske tiltak kan være hvitelisting (forhåndsgodkjenning av maskiner, MAC-adresser, IP-adresser, programvare, protokoller m.m.), multifaktor-autentisering av brukere, pålogging og kommunikasjon over sikret kanal, rettighets- og tilgangsstyring og andre tiltak som for eksempel begrensning i antall feilpålogginger før muligheten stenges, tidsbegrenset tilgang, overvåkning og logganalyse. Personelltiltak omfatter identifisering, klarering og autorisasjon, bakgrunnssjekk og godkjenning av kvalifikasjoner og egnethet; se også § 6-7.

Virksomheten må ha en prosedyre for å vurdere behov for brukertilgang og tilhørende risiko. Virksomheten må ha prosedyrer for å tildele, endre og slette tilgang og rettigheter i driftskontrollsystemet.



Veiledning

- NSM Grunnprinsipper for IKT-sikkerhet
 - o 1.3 Kartlegg brukere og behov for tilgang
 - o 2.2 Etabler en sikker IKT-arkitektur
 - o 2.4 Beskytt virksomhetens nettverk
 - o 2.5 Kontroller dataflyt
 - o 2.6 Ha kontroll på identiteter og tilganger

Standarder

- ISO/IEC 27019:2017 - Tiltak for informasjonssikring for virksomheter i kraftforsyningen
 - o 6.2.2 Teleworking
 - o 9.1.1 Access control policy
 - o 9.1.2 Access to networks and network services
 - o 9.2.1 User registration and de-registration
 - o 9.2.2 User access provisioning
 - o 9.2.3 Management of privileged access rights

- o 9.2.4 Management of secret authentication information of users
- o 9.2.5 Review of user access rights
- o 9.2.6 Removal or adjustment of access rights
- o 9.3.1 Use of secret authentication information
- o 9.4.1 Information access restriction
- o 9.4.2 Secure log-on procedures
- o 9.4.3 Password management systems
- o 9.4.4 Use of privileged utility programs
- o 9.4.5 Access control to program source code
- o 11.3.1 ENR – Equipment sited on the premises of other energy utility organizations
- o 11.3.2 ENR – Equipment sited on customer's premises
- o 11.3.3 ENR – Interconnected control and communication systems
- o 13.1.5 ENR – Logical connection of external process control systems
- IEC 62443-2-1 – Establishing an industrial automation and control system security program
 - o 4.3.2.6 Security policies and procedures
 - o 4.3.3.3 Physical and environmental security
 - o 4.3.3.4 Network segmentation
 - o 4.3.3.5 Access control – Account administration
 - o 4.3.3.6 Access control – Authentication
 - o 4.3.3.7 Access control – Authorization
- IEC 62443-3-3 – System security requirements and security levels
- NIST 800-82 rev2 - Guide to Industrial Control Systems (ICS) Security
 - o 6.2.1 Access Control
 - o 6.2.2 Awareness and training
 - o 6.2.7 Identification and Authentication
 - o 6.2.16 System and Communications Protection
- NERC CIP-004-6 Personnel and training
 - o R4 Access Control
- NERC CIP-007-6 System Security Management

7.11 Systemredundans i driftskontrollsystemet



§ 7-11. Systemredundans i driftskontrollsystemet

Virksomheter skal vurdere behovet for redundans i driftskontrollsystemet basert på lokale forhold og risikovurdering.

Ordforklaring

Redundans	Reservekapasitet/dublering av kritiske komponenter og funksjoner for å øke påliteligheten til systemet
------------------	--

Hvordan oppfylle kravet

Kravet betyr at virksomheten må vurdere behovet for redundans i driftskontrollsystemet. Vurderingen skal ta utgangspunkt i en risikovurdering av driftskontrollsystemet. Virksomheten må derfor kartlegge risiko for enkeltfeil og identifisere de tilfeller der enkeltfeil medfører uakseptabel konsekvens. I disse tilfellene skal redundans som forebyggende tiltak vurderes, men det er mulig å velge andre tiltak enn redundans.

Redundans kan oppnås ved å dublere kommunikasjonslinjer i risikoutsatte områder, ved å ha dubler kritiske komponenter eller prosessmaskiner. Redundans reduserer risikoen for alvorlig svikt i driftskontrollsystemet ved en enkelt feil i en enkelt komponent eller en maskin.

Dersom virksomheter med driftskontrollsystem i klasse 1 vurderer at det er behov for redundans, bør de iverksette tiltak som styrker redundansen. Dersom virksomheter med driftskontrollsystem i klasse 1 vurderer at det ikke er behov for redundans, er virksomheten likevel pålagt kompenserende tiltak i form av reparasjonsberedskap (se kapittel 4 og forskriftens vedlegg 1). For virksomheter i klasse 2 og 3 er kravet til redundans tydeligere, se § 7-14 g og h, og § 7-15 d.



Eksempel: Risikoanalysen viser behov for redundante kraftlinjer

Risikoanalysen til Kraftkonsernet AS viser at en av kraftlinjene går i et rasutsatt område. I dag er det bare en kraftlinje til klasse 2 transformatorstasjon som forsyner mange med strøm. Risikoanalysen konkluderer med at risikoen for ras vil øke i tiden framover som følge av klimatiske endringer. Kraftkonsernets ledelse beslutter derfor å bygge en alternativ kommunikasjonslinje til denne transformatorstasjonen som går utenfor rasområdet. De setter i gang et arbeid med å utrede radiolinje eller bruk av offentlig mobilnett som redundant kommunikasjon til transformatorstasjonen. På en annen strekning med kommunikasjon til en klasse 1 stasjon, er også risikoen høy. Her vurderer virksomheten å heller etablere reparasjonsberedskap.



Standarder

[NIST, Guide to Industrial Control Systems \(ICS\) Security](#)
[ISO/IEC 27019:2017 - Information technology — Security techniques — Information security controls for the energy utility industry](#)

Veiledning

[MSB, Guide to Increased Security in Industrial Control Systems](#)

Krysskoplinger til annet regelverk

Kbf §§ 2-3, 5-8 og 6-9c stiller krav til risikovurdering, som vurdering av redundans er en del av

Kbf § 2-10 Internkontroll.

Det kan være nyttig å se på kravene til redundans og dublering i vedlegg 2 og 3 til §§ 5-5 og 5-6 i forskriften. Vedleggene kommer bak i forskriften.

Klasse 2 og 3 driftskontrollsystemer har tilleggskrav om redundans i § 7-14 g.

Klasse 3 driftskontrollsystemer har tilleggskrav om redundans i § 7-15 a og d.

Kapittel 4s krav til reparasjonsberedskap

7.12 (Opphevet)

Denne paragrafen er opphevet 1.1.2019.

7.13 Beskyttelse mot elektromagnetisk puls og interferens

§

§ 7-13. Beskyttelse mot elektromagnetisk puls og interferens

Virksomheter skal vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls (EMP) eller elektromagnetisk interferens (EMI). Dersom sårbarheter avdekkes, skal det gjennomføres sikrings- eller beredskapstiltak etter driftskontrollsystemets betydning for sikker drift og gjenoppretting av funksjon i kraftforsyningen.

Ordforklaring

Elektromagnetisk puls (EMP)	EMP omfatter alle elektriske forstyrrelser med kort varighet. EMP transmitteres både som elektromagnetisk stråling og som ledningsbåren strømpuls. EMP fra lynutladninger omtales som LEMP (L = Lightning) og EMP fra kjerneeksplosjoner betegnes NEMP (N = Nuclear). NEMP er ca. 1000 ganger raskere enn LEMP
Elektromagnetisk interferens (EMI)	Elektromagnetisk interferens, betegnelse på forstyrrelser og støy i elektronisk utstyr som skyldes elektromagnetisk påvirkning fra omgivelsene, enten denne kommer i form av radiobølger eller via ledninger
Tilsiktet (intentional) elektro-	Elektromagnetisk forstyrrelse forårsaket av radiofrekvente våpen (RFV) med mikrobølgekilder. 18 GHz utgjør en øvre teoretisk grense for

magnetisk interferens (IEMI)	funksjonsforstyrrelser eller ødeleggelse av elektronisk utstyr, mens 10 GHz utgjør en øvre grense for praktisk utforming av radiofrekvente våpen. Virkningen dekker et meget begrenset geografisk område, i praksis kanskje bare opptil 100 m. Energien kan – på tilsvarende måte som for EMP – forplante seg som stråling eller være ledningsbundet. En smalspektret puls kan ha svært høy pulseffekt, selv om det totale energiinnholdet er lavt. Det største skadepotensialet ligger i utnyttelse av resonans. En bredspektret puls har mye lavere spektraleffekt, og er mer egnet til å skape forstyrrelser enn forårsake varig skade
-------------------------------------	---

Hvordan oppfylle kravet

Virksomheten skal vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls og elektromagnetisk interferens. Definisjonen av driftskontrollsystem er vid, jf. § 7-1.

Virksomheten må gjøre en samlet vurdering av risiko og behov for EMP- og EMI-sikring i driftskontrollsystemet. Basert på risikovurderingen må virksomheten ha en overordnet strategi for hvordan sikring gjennomføres. Et sentralt driftskontrollsystem som styrer mange lokalkontrollanlegg vil kreve høy driftspålitelighet (oppetid), mens andre mindre kritiske funksjoner, eksempelvis lokalkontrollanlegg, kan tillates å falle ut en kort tid. Andre igjen kan ha avbrudd noe lengre tid uten at det får konsekvenser for kraftforsyningen, eksempelvis dublert kommunikasjonsvei. Tiltak vil kunne være jording, skjerming, avledning og filtrering, alternativt reservedeler eller prosedyre for manuell styring direkte i kontrollanlegget.



Veiledning

[SINTEF Energiforskning. EMP-sikring av kraftforsyningsanlegg: Håndbok. Lysaker: Energiforsyningsens fellesorganisasjon, 2000](#)

Forsvarsbygg. *EMP-handbok: Veiledning i sikring av kritisk infrastruktur mot elektromagnetiske effekter*. Oslo: Forsvarsbygg, 2020. (Distribusjon ved henvendelse til Forsvarsbygg)

[Beskyttelse av elektroniske installasjoner i totalforsvaret mot elektromagnetisk puls \(EMP\), retningslinjer fastsatt av Samferdselsdepartementet 24.03.1998.](#)

Krysskoplinger til annet regelverk

Driftskontrollsystemer i klasse 2 og 3 har tilleggskrav om EMP og EMI i kbf § 7-14 i.

Driftskontrollsystemer i klasse 3 har tilleggskrav om EMP og EMI i kbf § 7-15 e.

7.14 Særskilte krav til driftskontrollsystemer i klasse 2

§

§ 7-14. Særskilte krav til driftskontrollsystem klasse 2

Foruten de generelle krav til beskyttelse av driftskontrollsystemet, skal virksomheter med driftskontrollsystem i klasse 2 oppfylle følgende tilleggskrav:

a. Sikkerhetskopier

Virksomheten skal jevnlig teste at gjenoppretting av elektroniske sikkerhetskopier fungerer etter hensikten

b. Sikkerhetsrevisjon

Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene faktisk er etablert og fungerer etter sin hensikt

c. Overvåking og logging

Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet

d. Utilgjengelig driftssentral

Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid.

e. Bemanning av driftssentral

Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold

Virksomheten skal senest innen én time kunne bemanne driftssentralen.

Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.

f. Ekstern tilkobling til driftskontrollsystemet

Ved tilkobling fra leverandører skal driftssentralen være bemannet

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 kraftforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person.

Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.

g. Systemredundans

Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett

Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans.

Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner.

Det skal etableres reparasjonsberedskap for alt samband, jf. kapittel 4 og § 7-8.

h. Særskilt om dublering

Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil ikke rammer alle dublerne samtidig, jf. § 7-7

i. Beskyttelse mot EMP og EMI

Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer

j. Sikker tidsreferanse

Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse

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

Hvordan oppfylle kravet

Kravene i bestemmelsen er detaljerte tilleggskrav til klasse 2 driftskontrollsystemer. Disse kravene kommer i tillegg til grunnkrav som er oppstilt tidligere i kapittel 7 i forskriften.

Bokstav a

§ 7-14a. Sikkerhetskopier gjelder elektroniske sikkerhetskopier som kan brukes til å gjenopprette systemet etter ekstraordinær hendelse, for eksempel utilsiktet systemsvikt eller angrep med krypteringsvirus. Sikkerhetskopiene må lagres trygt og være beskyttet mot all ikke autorisert endring. Prosedyre for testing av sikkerhetskopier bør inngå i internkontrollsystemet og testing bør gjøres minimum årlig. Kravet bygger videre på § 7-8, se også § 4-1 Reparasjonsberedskap, § 7-3 Dokumentasjon av driftskontrollsystemet og § 6-8 Sikkerhetskopier.

Bokstav b

§ 7-14 b. Sikkerhetsrevisjon skal gjennomføres jevnlig for å teste at pålagte tiltak faktisk er etablert og fungerer. NVE anbefaler at sikkerhetsrevisjon gjøres årlig og inngår i virksomhetens årsplan.

Bokstav c

Overvåkning og logging bygger på § 7-7. Logger knyttet til brukeraktivitet bør lagres i minst 2 år av hensyn til etterforskning av uønskede hendelser der en angriper kan skjule sin aktivitet i systemet i lengre tid. Hensikten med bestemmelsen er at virksomheten ved tidlig varsling til KraftCERT (se § 6-9 bokstav c) om uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet kan hindre tap av funksjon i driftskontrollsystemet eller få satt i gang feilsøking og feilretting raskest mulig.

Virksomheten må ha et system som automatisk overvåker trafikk i nettverk og som gir alarm eller varsler ved unormal aktivitet. Bestemmelsen må ses i sammenheng med kravet om å etablere effektive reaksjonsrutiner for å håndtere feil, sårbarheter og sikkerhetsbrudd i driftskontrollsystemet i § 7-7. Håndtering av feil, sårbarheter og sikkerhetsbrudd.

Installering, konfigurering og innstillinger av alarmer og monitoreringsparametre i overvåkingssystem eller i brannmurer eller svitsjer kan være komplisert, og øker i kompleksitet med størrelse og omfang på driftskontrollsystemet. Blir systemene konfigurert feil, risikerer man å få mange falske alarmer, men også at systemene stopper «lovlig» trafikk i driftskontrollsystemet eller ikke beskytter systemet som tiltenkt.

NVE anbefaler at virksomheten samarbeider med leverandøren av driftskontrollsystemet når virksomheten skal etablere automatiske overvåkings- eller beskyttelsessystem i driftskontrollsystemet. På den måten kan man unngå at funksjonalitet i driftskontrollsystemet blir forstyrret eller hindret ettersom overvåkingssystemene også kan forstyrre normal datatrafikk.

Hvis systemet krever at man utplasserer sensorer i nettverket, må man passe på at disse ikke forstyrrer signalene for å overvåke og styre anleggene. En måte å gjøre det på, kan være å plassere sensorer utenfor selve driftskontrollsystemet slik at man ikke foretar analyse i datanettverket til driftskontrollsystemet.

Bokstav d

Virksomheter med klasse 2 driftssentraler skal kunne drifte systemet selv om driftssentralen blir utilgjengelig. Kravene bygger videre på kravet i § 7-8 Beredskap ved svikt i driftskontrollsystemet og gir flere føringer for løsningen.

Bokstav e

Bestemmelsen stiller detaljert krav til bemanning og styrking av driftssentral i klasse 2 driftskontrollsystemer. Kravet kommer i tillegg til § 7-9 Bemanning av driftssentral.

Bokstav f

Ekstern tilkopling til driftskontrollsystemet er tilleggskrav til § 7-10 Ekstern tilkopling. Kravene er detaljerte og gir flere føringer. Virksomheten må selv vurdere hva som er tilstrekkelig sikre omgivelser og sikkert sted. NVE vurderer offentlig rom (flyplasser, kjøpesentre, hoteller) som ikke-sikkert sted, fordi det ikke er begrensninger med hensyn til hvem som kan ha adgang. Dersom en må koble til driftskontrollsystemet utenfor leverandørens eller virksomhetens lokaler, er det viktig at det er iverksatt gode sikringstiltak som beskytter både opp- og nedkobling, samt overføring av data, mot avlytting og manipulasjon.

Bokstav g

Systemredundans kommer som tilleggskrav til § 7-11. Mens § 7-11 setter krav til å vurdere behovet og velge aktuelle tiltak for å håndtere risikoen, så er kravene i § 7-14g detaljkrav som styrker sikkerheten og begrenser valgfriheten. Kravet er spesielt strengt når det gjelder samband og redundans. Samband

skal fungere uavhengig av svikt i det offentlige elektroniske kommunikasjonssystemer. NVE godtar at en sambandsvei i en redundant løsning går via offentlige elektroniske kommunikasjonsnett.

Bokstav h

Bestemmelsen bygger også videre på § 7-11 og detaljerer krav til å redusere risikoen for at samme feil rammer redundante systemer. Kravet er at sikringstiltak skal hindre at en feil, eksempelvis skadevare, smitter på reservesystemet. Dersom en ikke benytter ulike teknologier fra for eksempel ulike leverandører, må risikoen håndteres gjennom andre forebyggende tekniske og organisatoriske sikringstiltak. Eksempler er rutiner for uttesting av programvare før oppdatering, sikkerhetskopier, planlagt og testet backup, reserveløsninger og prosedyrer for manuell drift.

Bokstav i

Bestemmelsen bygger videre på § 7-13 og setter i tillegg krav til EMP- og EMI-sikring av minst en sambandsvei fra driftskontrollsystemet til anlegg i klasse 2 og 3.

All elektronikk, inkludert sambandsutstyr og datautrustning tilhørende driftskontrollsystemer, er i utgangspunktet meget sårbart for ekstreme elektromagnetiske hendelser som HEMP og IEMI. Kraftkomponenter (transformatorer mv), vern og instrumentering er langt mer hardføre, men overgangen til digitalt instrumenterte transformatorstasjoner i friluft, gir sårbarhet for vern og instrumentering. EMP- og EMI-beskyttelse vil begrense skadevirkningene dersom trusselen inntreffer.

Behovet for beskyttelse mot HEMP E1 er minimum 30 dB demping for frekvenser opp til 1 GHz. Behovet for beskyttelse mot HEMP E1 og IEMI kombinert er minimum 30 dB demping for frekvenser opp til 10 GHz.

Beskyttelsesnivået vil ikke forhindre funksjonsfeil, forstyrrelser og mulig avbrudd, men forhindre varig skade på elektronisk utstyr og datautrustning.

Anlegg med fjelloverdekning på minst 10 meter er naturlig sikret mot strålingsfelt fra HEMP E1 og IEMI, men behovet for vern mot transiente overspenninger på kabler og ledningsnett må vurderes.

HEMP vil ramme mange anlegg samtidig. Beskyttelsen består i et tilstrekkelig robust kraftsystem som kan motstå skadevirkningene. IEMI er derimot en mulig trussel kun mot enkeltanlegg eller deler av driftskontrollsystemet. IEMI-trusselen kan antas å være størst for de mest kritiske anleggene, og mest relevant for anlegg med fri sikt og enkel adkomst med kjøretøy. Sårbarheten for IEMI-trusler er avhengig av redundansen i kraftsystemet, antatt skadeomfang og medgått tid for gjenoppretting av systemredundans.

Krav om beskyttelse mot HEMP E1 omfatter i utgangspunktet alle installasjoner i driftskontrollsystemer i klasse 2 og 3, og alle lokalkontrollanlegg for kraftforsyningsanlegg i klasse 2 og 3. Tilleggsbeskyttelse mot IEMI bør omfatte alle installasjoner i driftskontrollsystemer og lokalkontrollanlegg med fri sikt og enkel adkomst.

Tiltakene omfatter skjerming, jording og avledning, eventuelt i kombinasjon med soneinndeling. For planlegging, utførelse og testing henvises til relevante standarder og veiledere nedenfor.

**EMP-sikring vil vanligvis måtte omfatte:**

- Lokalkontrollanlegg for kraftforsyningsanlegg i klasse 2 og 3
- Minst én sambandsvei til kraftforsyningsanlegg i klasse 2 og 3. For sambandsvei til kraftforsyningsanlegg i klasse 2 kan EMP-beredskap aksepteres
- Datarom, sambandsrom og driftssentral (kontrollrom) for driftskontrollsystemer i klasse 2 og 3, inkludert systemer for sikkerhetskopiering og løsninger/installasjoner for alternativ drift. Utstyr som ikke befinner seg i EMP-sikre rom, må kunne erstattes raskt av utstyr som ikke er påvirket av den samme hendelsen
- Nødstrømsforsyning skal være EMP-sikret; under og etter en EMP- eller EMI-hendelse skal nødstrømanlegget inklusiv aggregatet virke.
- Adgangskontrollsystemer og systemer for elektronisk overvåkning

**Maler****Standarder****IEC 61000 serien om elektromagnetisk kompatibilitet**

IEC/TR 61000-1-3:2002: Electromagnetic compatibility (EMC) – Part 1-3: General – The effects of high-altitude EMP (HEMP) on civil equipment and systems.

IEC/TR 61000-1-5:2004: Electromagnetic compatibility (EMC) – Part 1-5: General – High power electromagnetic (HPEM) effects on civil systems.

IEC 61000-2-9:1996: Electromagnetic compatibility (EMC) – Part 2: Environment – Section 9: Description of HEMP environment – Radiated disturbance.

IEC 61000-2-10:1998: Electromagnetic compatibility (EMC) – Part 2-10: Environment – Description of HEMP environment – Conducted disturbance

IEC 61000-2-11:1999: Electromagnetic compatibility (EMC) – Part 2-11: Environment – Classification of HEMP environments.

IEC 61000-2-13:2005: Electromagnetic compatibility (EMC) – Part 2-13: High-power electromagnetic (HPEM) environments – Radiated and conducted.

IEC 61000-4-23:2016: Electromagnetic compatibility (EMC) – Part 4-23: Testing and measurement techniques – Test methods for protective devices for HEMP and other radiated disturbances.

IEC 61000-4-24:2015: Electromagnetic compatibility (EMC) – Part 4-24: Testing and measurement techniques – Test methods for protective devices for HEMP conducted disturbance.

IEC 61000-4-25:20012001+A1:2012+A2:2019: Electromagnetic compatibility (EMC) – Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems.

IEC/TR 61000-4-32:2002: Electromagnetic compatibility (EMC) – Part 4-32: Testing and measurement techniques – High-altitude electromagnetic pulse (HEMP) simulator compendium.

IEC 61000-4-33:2005: Electromagnetic compatibility (EMC) – Part 4-33: Testing and measurement techniques – Measurement methods for high-power transient parameters.

IEC/TR 61000-4-35:2009: Electromagnetic compatibility (EMC) – Part 4-35: Testing and measurement techniques – High power electromagnetic (HPEM) simulator compendium.

IEC 61000-4-36:2020: Electromagnetic compatibility (EMC) – Part 4-36: Testing and measurement techniques – IEMI immunity test methods for equipment and systems.

IEC/TR 61000-5-3:1999: Electromagnetic compatibility (EMC) – Part 5-3: Installation and mitigation guidelines – HEMP protection concepts.

IEC/TS 61000-5-4:1996: Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 4: Immunity to HEMP – Specifications for protective devices against HEMP radiated disturbance.

IEC 61000-5-5:1996: Electromagnetic compatibility (EMC) – Part 5: Installation and mitigation guidelines – Section 5: Specification of protective devices for HEMP conducted disturbance.

IEC/TR 61000-5-6:2002: Electromagnetic compatibility (EMC) – Part 5-6: Installation and mitigation guidelines – Mitigation of external EM influences.

IEC 61000-5-7:2001: Electromagnetic compatibility (EMC) – Part 5-7: Installation and mitigation guidelines – Degrees of protection by enclosures against electromagnetic disturbances (EM code).

IEC/TS 61000-5-8:2009: Electromagnetic compatibility (EMC) – Part 5-8: Installation and mitigation guidelines – HEMP protection methods for the distributed infrastructure.

IEC/TS 61000-5-9:2009: Electromagnetic compatibility (EMC) – Part 5-9: Installation and mitigation guidelines – System-level susceptibility assessments for HEMP and HPEM.

IEC/TS 61000-5-10:2017: Electromagnetic compatibility (EMC) – Part 5-10: Installation and mitigation guidelines – Guidance on the protection of facilities against HEMP and IEMI.

IEC 61000-6-6:2003: Electromagnetic compatibility (EMC) – Part 6-6: Generic standards – HEMP immunity for indoor equipment.

Veiledere

[SINTEF Energiforskning. EMP-sikring av kraftforsyningsanlegg: Håndbok. Lysaker: Energiforsyningens fellesorganisasjon, 2000](#)

Forsvarsbygg. *EMP-handbok: Veiledning i sikring av kritisk infrastruktur mot elektromagnetiske effekter*. Oslo: Forsvarsbygg, 2020. (Distribusjon ved henvendelse til Forsvarsbygg)

[Beskyttelse av elektroniske installasjoner i totalforsvaret mot elektromagnetisk puls \(EMP\), retningslinjer fastsatt av Samferdselsdepartementet 24.03.1998](#)

Krysskopling til annet regelverk

§ 7-13 Beskyttelse mot elektromagnetisk puls og interferens

Bokstav j

Bestemmelsen setter krav til sikre kilder for tidsangivelse.

Kraftsystemets funksjoner og tilstander kan ha behov for synkronisert tid i driftskontrollsystemet, blant annet for registrering av feil i kraftsystemet og pålitelig drift av datasystemer og kontrollanlegg.

Behovet for nøyaktighet er moderat (~ 10 ms), så lenge hensikten med systemtiden er begrenset til å synkronisere de ulike komponentene (tjenere, PCer, rutere, brannmurer, dataskjerm mv) i driftskontrollsystemet. Behovet øker (~ 1 ms) når måleverdier og hendelser i kraftsystemet skal ha tidsstempel. Først med instrumentering og digital styring i henhold til IEC 61850 er synkronisering av datastrømmer og enheter et ubetinget krav. Ikke-konvensjonelle instrumenteringsløsninger og dynamisk systemovervåkning med høyoppløste digitale måleverdistrømmer krever eventuelt en nøyaktighet på bedre enn 1 μ s.

Den langt vanligste tidskilden i norske kraftforsyningsanlegg og driftskontrollsystemer er direkte synkronisering ved bruk av GPS-mottakere. Spesielt relevant er derfor å redusere sårbarheten ved tap av GPS-signal.

Også atmosfæriske forhold kan forårsake tap eller degradering av GPS-signaler over et større geografisk område.

GPS-mottakere med integritetsfunksjon gjør bruk av informasjon fra flest mulig satellitter for å vurdere gyldigheten av signalene. GPS-mottakere uten integritetsfunksjon er sårbare for støysendinger, og kan vanskelig skille mellom ekte og falske GPS-signaler.

Radiointerferens kan være utilsiktet eller tilsiktet. Ved mistanke om utilsiktet radiointerferens, må den nasjonale frekvensmyndigheten (NKOM) <https://www.nkom.no/> kontaktes, slik at kilden kan avdekkes og fjernes. Se ellers §§ 2-5 og 2-6.

Selv om driftskontrollsystemet hos en KBO-enhet ikke er avhengig av nøyaktig tid, så vil bortfall eller feilvisning av tid få driftsmessige konsekvenser. KBO-enheten bør derfor vurdere risiko og eventuelt treffe passende tiltak.

De GPS-mottakerne som er mest utbredt i kraftforsyningen, leveres med kvartsklokker, og er utstyrt med kun enkle antenner og har få muligheter for konfigurering. KBO-enhetene bør vurdere om de vanligste mottakerne er tilstrekkelig sikre og nøyaktige.

Mulige tiltak er å:

- Utstyre GPS-mottakerne med bedre antenner som gir større signal og mindre støy-forhold. Dermed vil GPS-mottakerne bli mer resistente mot støysendinger og andre forstyrrelser av signalmottaket, herunder romvær og atmosfæriske forstyrrelser
- Konfigurere stasjonære GPS-mottakere med sin sanne posisjon, og sørge for alarm når posisjonsestimatet havner utenfor unøyaktighetsrommet
- Installere redundante mottakere, fordelt på GPS og Galileo. En viktig faktor er at GPS og Galileo benytter ulike frekvenser
- Samle inn og overvåke navigasjonsmeldingene som GPS-mottakerne behandler. Dermed kan eventuelle falske kodestrømmer avdekkes, og alarm gis
- Utstyre GPS-mottakerne med mer nøyaktige klokker slik at utfall av GPS-signaler kan tolereres over lengre tidsrom
- Ved bruk av GPS-klokker, ha tre kilder slik at dersom en klokke feiler, kan fortsatt to gi korrekt tid
- Andre klokker, for eksempel atom-ur



Standarder

IEC 61850-9-2:2011+A1:2020: Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3

IEC TR 61850-90-4:2013: Communication networks and systems for power utility automation - Part 90-4: Network engineering guidelines

IEC/IEEE 61850-9-3:2016: Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation

Veiledere

Norsk Romsenter, Vurdering av sårbarhet ved bruk av globale satelittnavigasjonssystemer i kritisk infrastruktur, Oslo, mars 2013.

Bokstav k

Krav til leverandører

Her settes krav til hvilke leverandører som får levere systemer til norsk kraftforsyning. Kravet gjelder komplette leveranser til driftskontrollsystemet, og ikke enkeltstående komponenter som utgjør en del av en helhet. Store globale leverandører har produksjon og forskning lokalisert i ulike deler av verden, og de er avhengige av leverandører og underleverandører. Å utelukke enkeltkomponenter er derfor ikke gjennomførbart i praksis. En sikker kraftforsyning inngår i NATOs sju basiskrav til vertsnasjoner som mottar NATO-støtte. Når det gjelder anskaffelse av driftskontrollsystemer er anskaffelse foretatt nært opp til sikkerhetslovens krav derfor å foretrekke. For virksomheter som ikke er underlagt sikkerhetsloven, vil dette kravet sammen med § 6-6 Begrenset anbudsinnbydelse gi virksomhetene noen verktøy. For ordens skyld presiserer vi at bestemmelsen ikke er ment å utelukke norske leverandører.

7.15 Særskilte krav til driftskontrollsystem klasse 3

§

§ 7-15. Særskilte krav til driftskontrollsystem klasse 3

Foruten de generelle kravene samt særskilte krav til beskyttelse av driftskontrollsystem i klasse 2, skal virksomheter med driftskontrollsystem i klasse 3 oppfylle følgende tilleggskrav:

a. **Reserve driftssentral**

Virksomheter skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge.

Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner.

Virksomheter skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, annet ledd.

b. **Bemanning av driftssentral**

Driftssentralen skal være døgnbemannet.

Opptrapping av bemanningen skal kunne skje innen én time etter at påkalling er gjort.

Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, andre ledd.

c. **Ekstern tilkobling til driftskontrollsystemet**

Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.

d. **Systemredundans**

Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem.

Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf. kapittel 5.

e. **Beskyttelse mot EMP og EMI**

Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak.

I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.

f. **Fastsettelse av særlige krav til bemanning**

For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf. § 5-7.

Hvordan oppfylle kravet

Kravene i §7-15 er detaljerte tilleggskrav til klasse 3 driftskontrollsystemer. Disse kravene kommer i tillegg til grunnkrav som er oppstilt tidligere i kapittel 7 i forskriften og krav som er stilt til klasse 2 driftskontrollsystemer i § 7-14.

Bokstav a

Bestemmelsen stiller krav til en operativ fysisk reservedriftssentral som virksomheten kan ta i bruk på kort varsel. Den skal plasseres i så lang avstand at samme hendelse ikke rammer begge sentralene. Med hendelser mener NVE ekstraordinære hendelser, se ellers § 2-5 for eksempel på hendelser. Sentralen må derfor ha egnet utstyr og tilstrekkelig bemanning i tillegg til egen fysisk lokasjon. Redundanskravet til servere, front-end og samband kan oppfylles ved at ett system er plassert på samme sted som driftssentralen, og det andre systemet der reservedriftssentralen er plassert.

Bokstav b

Bestemmelsen stiller krav til kapasitet (døgnbemannet) og å være operativ med økt kapasitet innen en time. Bemanningsbehovet skal vurderes minimum årlig.

Bokstav c

Bestemmelsen setter et tydelig forbud mot å kople eller styre øvrige anlegg gjennom ekstern tilkopling utenom driftssentralen. Det er forbud mot å styre nett og prosesser hjemmefra.

Bokstav d

Bestemmelsen skjerper ytterligere kravene til redundans i sambandsveiene i driftskontrollsystemet, både med hensyn til innbyrdes separasjon av sambandsveier og med hensyn til at virksomheten selv skal ha kontroll over minst én sambandsvei som også er sikret iht. kravene i kapittel 5.

Bokstav e

Bestemmelsen setter krav til EMI/EMP-sikringstiltak, og bygger videre på § 7-13 og § 7-14 bokstav i.

Tilleggskrav til klasse 3 driftskontrollsystem (Merk! Kravene til klasse 2 gjelder også)

Grunnkrav	Tilleggskrav klasse 2 og 3 § 7-14	Ytterligere tillegg for klasse 3 § 7-15
§ 7-1	Foruten de generelle krav til beskyttelse av driftskontrollsystemet, skal virksomheter med driftskontrollsystem i klasse 2 oppfylle følgende tilleggskrav:	Foruten de generelle kravene samt særskilte krav til beskyttelse av driftskontrollsystem i klasse 2, skal virksomheter med driftskontrollsystem i klasse 3 oppfylle følgende tilleggskrav:
§7-8	a. <i>Sikkerhetskopier</i> Virksomheten skal jevnlig teste at gjenoppretting av elektroniske sikkerhetskopier fungerer etter hensikten.	
§ 7-2	b. <i>Sikkerhetsrevisjon</i> Virksomheten skal jevnlig gjennomføre en sikkerhetsrevisjon og kontroll av pålagte beskyttelsestiltak i driftskontrollsystemet. Revisjonens formål skal være å påse at tiltakene	

Grunnkrav	Tilleggskrav klasse 2 og 3 § 7-14	Ytterligere tillegg for klasse 3 § 7-15
	faktisk er etablert og fungerer etter sin hensikt.	
§ 7-4	c. <i>Overvåking og logging</i> Virksomheten skal ha automatisk overvåking, logging, analyse og varsling ved uautorisert bruk, forsøk på uautorisert tilgang, unormal datatrafikk eller annen aktivitet som ikke er autorisert i driftskontrollsystemet.	
§ 7-8	d. <i>Utilgjengelig driftssentral</i> Dersom driftssentralen blir utilgjengelig, skal virksomheten kunne betjene og manuelt styre anlegg som inngår i virksomhetens driftskontrollsystem. I tillegg skal virksomheten ha planer for alternativ drift dersom driftssentralen blir utilgjengelig over lengre tid.	a. <i>Reserve driftssentral</i> Virksomheter skal ha reserve driftssentral som skal plasseres i sikker avstand til ordinær driftssentral, slik at ikke samme hendelse kan ramme begge. Reserve driftssentral skal til enhver tid være klar til bruk og være utstyrt slik at den kan fungere helt uavhengig av ordinær driftssentral og kunne ivareta alle driftskontrollfunksjoner. Virksomheter skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, annet ledd.
§ 7-9	e. <i>Bemanning av driftssentral</i> Virksomheten skal sørge for at alle påregnelige ekstraordinære situasjoner eller hendelser i energisystemet eller i driftskontrollsystemet umiddelbart oppdages og håndteres uten unødig opphold. Virksomheten skal senest innen én time kunne bemanne driftssentralen. Virksomheten skal ha en vaktordning som til enhver tid sikrer rask opptrapping av bemanningen ved behov.	b. <i>Bemanning av driftssentral</i> Driftssentralen skal være døgnbemannet. Opptrapping av bemanningen skal kunne skje innen én time etter at påkalling er gjort. Virksomheten skal minimum årlig vurdere om det er behov for å øke bemanningen eller omfanget av vaktordningen for rask opptrapping av bemanning, jf. § 7-9, andre ledd. f. <i>Fastsettelse av særlige krav til bemanning</i> For spesielt viktige driftskontrollsystemer kan beredskapsmyndigheten fastsette særlige krav, også til bemanning, jf. § 5-7.
§ 7-10	f. <i>Ekstern tilkobling til driftskontrollsystemet</i> 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	c. <i>Ekstern tilkobling til driftskontrollsystemet</i> Kobling i nettanlegg eller styring av øvrige anlegg gjennom ekstern tilkobling er ikke tillatt.

Grunnkrav	Tilleggskrav klasse 2 og 3 § 7-14	Ytterligere tillegg for klasse 3 § 7-15
	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 kraftforsyningen gjennom ekstern tilkobling, skal styringen kun skje etter tillatelse eller retningslinjer fra bemyndiget person. Enhver påkobling til driftskontrollsystemet gjennom ekstern tilkobling skal loggføres.	
§ 7-11	g. <i>Systemredundans</i> Samband i driftskontrollsystemet skal fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett. Driftskontrollsystemet frem til anlegg i klasse 2 og 3 skal være redundant frem til det lokale kontrollanlegget. I det lokale kontrollanlegget skal virksomheten vurdere behovet for redundans. Redundante føringsveier for samband og redundante komponenter i driftskontrollsystemet skal være fysisk adskilte og uavhengige slik at én enkelt feil eller hendelse ikke medfører tap av viktige funksjoner. Det skal etableres reparasjonsberedskap for alt samband, jf. kapittel 4 og § 7-8.	d. <i>Systemredundans</i> Sambandsveiene i driftskontrollsystemet skal utføres så sikre og robuste og med en slik redundans og avstand at ikke samtidige eller påfølgende hendelser som uvær, brann eller omfattende teknisk svikt hindrer eller skader begge føringsveier og andre redundante delsystem. Frem til alle anlegg i klasse 3 skal virksomheten ha kontroll og råderett over alle komponenter og andre tekniske løsninger i minst én sambandsvei, og beskytte disse, jf. kapittel 5.
§ 7-10	h. <i>Særskilt om dublering</i> Ved dublering som benytter identiske teknologier og løsninger i driftskontrollsystemet, må virksomheten innrette seg slik at samme systemfeil ikke rammer alle dublerte system samtidig	
§ 7-13	i. <i>Beskyttelse mot EMP og EMI</i> Det skal gjennomføres sikrings- eller beredskapstiltak for beskyttelse av	e. <i>Beskyttelse mot EMP og EMI</i>

Grunn-krav	Tilleggskrav klasse 2 og 3 § 7-14	Ytterligere tillegg for klasse 3 § 7-15
	utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 2 og 3 som driftskontrollsystemet styrer.	Det skal gjennomføres sikringstiltak for beskyttelse av utrustning som nevnt i § 7-13 mot EMP og EMI for minst én sambandsvei til anlegg i klasse 3 som driftskontrollsystemet styrer. Beredskapsmyndigheten kan i særskilte tilfeller godkjenne beredskapstiltak som alternativ til sikringstiltak. I sambandsvei til anlegg i klasse 2 som driftskontrollsystemet styrer, skal det gjennomføres sikrings- eller beredskapstiltak.
	j. <i>Sikker tidsreferanse</i> Driftskontrollsystem som er avhengig av eksakt tidsreferanse, skal ha sikre kilder for tidsangivelse.	
	k. <i>Krav til leverandører</i> 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.	

7.16 Vern av kraftsystem i regional- og transmisjonsnett

§

§ 7-16. Vern av kraftsystem i regional- og transmisjonsnett

Kommunikasjonsbaserte vernsystemer i transmisjons- og regionalnett skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftsystemet.

Vernsystemet kan være en del av driftskontrollsystemet, eller bruke de samme kommunikasjonsveiene. Bestemmelsen inneholder ikke krav om at det skal etableres vern, kun om sikkerheten i vernkommunikasjonen og at feil skal frakobles raskt og selektivt. Bestemmelser i kapittel 7 gjelder for vernsystemene med utgangspunkt i driftskontrollsystemets eller lokalkontrollsystemets klasse.

Bestemmelsen stiller krav til sikring av elektronisk kommunikasjon i viktige vernsystemer, herunder fjerninnstilling av vern, og at vernsystemet skal ha innebygde egenskaper som begrenser konsekvensene av feil i vernet.

Kommunikasjonen innbyrdes mellom vern, og mellom en servicetekniker eller applikasjon som skal fjern-innstille vern, må være sikret mot ikke godkjent tilgang og ikke godkjent endring.

I forskriftsbestemmelsene til systemansvarsforskriften og forskrift om elektriske forsyningsanlegg er det krav om å ha fungerende vernsystemer.

I Statnetts veiledning NVF 2020 finnes detaljerte bestemmelser om vernfunksjonalitet med tilhørende krav.



Veiledere

Statnett NVF 2020 Nasjonal veileder for funksjonskrav i kraftsystemet
DSB [Forskrift om elektriske forsyningsanlegg](#) (FEF)

Krysskoplinger til annet regelverk

[Forskrift om systemansvaret i kraftsystemet](#) § 20. *Vern og reléplanlegging* og i § 21. *Systemvern*.

[FEF § 2-11. Overvåking og kontrollsystemer](#)

[FEF § 4-10. Vern, kontroll og hjelpesystemer](#)

§ 7-10. Ekstern tilkobling til driftskontrollsystem

§ 7-11. Systemredundans i driftskontrollsystemet

§ 7-13. Beskyttelse mot elektromagnetisk puls og interferens

§ 7-14. Særskilte krav til driftskontrollsystem klasse 2

§ 7-15. Særskilte krav til driftskontrollsystem klasse 3

7.17 Mobile radionett – driftsradio



§ 7-17. Mobile radionett – driftsradio

KBO-enheter som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon, skal ha tilgang til et mobilt sambandssystem. Dette sambandssystemet skal:

- a. Omfattes av den generelle sikringsplikten etter § 5-1
- b. Til enhver tid holdes i funksjonsdyktig stand, være klar til bruk, og det skal være rask tilgang på kritiske reservedeler og kompetanse på feilretting
- c. Kunne betjenes av personell med nødvendig kompetanse til bruk
- d. Ha tilstrekkelig dekningsgrad for kraftforsyningens anlegg og drift
- e. Kunne fungere uavhengig av funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett
- f. Ha tilstrekkelig nødstrøm ved omfattende eller langvarige strømbrudd, herunder et nødstrømssystem med automatisk start og minimum 48 timer selvstendig driftstid
- g. Ha nødvendig funksjonalitet med blant annet direkte apparat til apparat-kommunikasjon, gruppesending og felles oppkall
- h. Kunne fungere som reservesamband om annet viktig samband svikter
- i. Der hvor radionettet benytter anlegg tilhørende et klassifisert driftskontrollsystem eller hvor det må regnes som en del av dette, skal sambandssystemet beskyttes i henhold til driftskontrollsystemets klasse
- j. Der hvor radionettet er digitalisert og f.eks. baserer seg på IP-løsninger, skal dette sikres mot uautorisert tilgang, spredning av uønsket programvare, urettmessig overtakelse m.m. etter relevante bestemmelser i denne forskrift

Hvordan oppfylle kravet

Hensikten med bestemmelsen er å sikre at de virksomhetene som er avhengige av et mobilt radionett, anskaffer et system som også fungerer i ekstraordinære situasjoner, for eksempel der forsyning av elektrisitet til et område faller ut.

Bestemmelsen om mobilt radionett er teknologinøytral. NVE setter ingen begrensninger for valg av system eller teknologi så lenge kravene i bestemmelsen og andre relevante krav i denne forskriften er oppfylt.

KBO-enheten må sikre uavhengighet i forhold til funksjonssvikt i offentlige elektroniske kommunikasjonstjenester eller kommunikasjonsnett. Nødstrøm for 3 døgns drift er et tiltak som kan bidra til det. Dersom tjenesten driftsradio kjøpes fra ekstern leverandør, må tjenesten ved strømafbrytning og brytning til sentral server hos leverandør tilby kommunikasjon i form av minimum talesamband mellom KBO-enhetens mannskap på anlegg ute og driftssentralen i minimum 48 timer.

Driftsradioen må ha tilstrekkelig geografisk dekningsgrad. Det betyr at mannskap hos KBO-enheten må kunne kommunisere med driftssentralen og utføre arbeid på alle viktige elkraftanlegg som KBO-enheten har ansvar for. KBO-enheten må ha oversikt over hvilke anlegg som er viktige for å

opprettholde forsyningssikkerhet. Dersom det ikke er dekning på stedet der mindre viktige anlegg står, må det være mulig å forflytte seg til et dekningsområde innenfor rimelig tid. Hva som er rimelig tid, avgjøres av KBO-enheten.

Systemet må som et minimum gi tilgang til talekommunikasjon mellom KBO-enhetens mannskap ute og driftssentralen selv om det offentlig ekom-nettet svikter. Risiko for svikt i radionettet reduseres ved å sikre at radionettet har tilstrekkelig nødstrøm for minimum 48 timer i områder der viktige elkraftanlegg er lokalisert. Dersom tjenesten kjøpes eksternt av leverandør, må virksomheten undersøke hvilke tjenester eller dekningsområde i radionettet som faller ut dersom driftsradioen mister kontakt med sentral server hos leverandøren, eller dersom offentlig ekom-nett faller ut. KBO-enheten må avhengig av konsekvensene, iverksette kompenserende tiltak.

Mobilt radionett blir normalt ikke klassifisert og er som sådan ikke en del av et klassifisert driftskontrollsystem, da det nødvendigvis ikke er sammenheng mellom driftskontrollsystemets betydning og radionettets betydning. Dersom KBO-enheten likevel, i tillegg til talekommunikasjon, benytter radiosystemet til overføring av signaler til driftskontrollsystemet eller andre viktige signaler, må KBO-enheten i tillegg oppfylle relevante krav til beskyttelse av driftskontrollsystemet i henhold til bestemmelsene. Dette gjelder særlig krav til redundans, særskilte krav til fysisk beskyttelse, EMP og EMI samt beskyttelse mot IKT-trusler. KBO-enheten bør også vurdere redundans ved for eksempel å ha to overføringsmuligheter i viktige dekningsområder, uavhengig om man benytter radiosystemet til andre formål enn talesamband. NVE anser ringstruktur av basestasjoner som et akseptabelt redundanstiltak.



Sjekkliste for mobil driftsradio

Strømforsyning og kabling

Ordinær strømforsyning, nødstrøm og samband bør føres inn i bygninger gjennom jordkabler. Stasjonens kabling bør organiseres slik at den beskytter mot overspenninger. Sikringsskap og liknende plasseres innendørs. Likerettere bør dupliseres og overvåkes med alarmer. Stasjonene bør utstyres med batterianlegg med driftstid på minst 72 timer. Alternativt kan stasjonen ha batterianlegg med driftstid på minst 48 timer dersom stasjonært nødstrømsaggregat er installert. Krav til nødstrøm kan reduseres dersom man har god adkomst til stasjonen.

Fysiske sikringstiltak

- Viktige og utsatte stasjoner bør bygges i betong, eventuelt stålkontainer (dette gir bl.a. beskyttelse mot brann, innbrudd og hærverk)
- Viktige komponenter bør plasseres i avlåste rom uten vinduer, med innbruddsalarm til døgnbemannet sentral (eventuelt hjemmevakt)
- Vinduer bør tildekkes med solide lemmer, låst eller boltet til innsiden
- Kabelføringer til mast bør føres i tildekket kanal eller i kabelbro slik at de ikke er lett tilgjengelige for uvedkommende
- Jordkabler bør beskyttes mekanisk ved at de legges i egne rør eller betongkanaler
- Antenner og master er vanskelige å beskytte. Her bør det anskaffes reserveutstyr og også tilrettelegge for alternative føringsveier for kommunikasjon. Master bør beskyttes med klatrehindre

- ARom som inneholder elektronisk utstyr og som har betydning for driften av driftsradiostasjonen (datarom og liknende), skal gjennom en risikovurdering vurderes skjermet mot EMP/EMI, jf § 7-13. *Beskyttelse mot elektromagnetisk puls og interferens*

Beskyttelse av digitale sambandsløsninger

Digitale driftsradioløsninger er utsatt for samme type trusler som annen IKT. Kravene i kapittel 6 og i kapittel 7 gjelder dersom radiosystemet også benyttes til signalering i driftskontrollsystemet.

Reservedeler og reparasjonsberedskap

Virksomhetens beredskapsplan må inkludere reparasjon av driftsradioanlegg. Virksomheten bør ha de mest kritiske komponentene i radiosystemet på lager. Der det benyttes viktige enheter med svært lang leveringstid, bør leverandøren kontaktes for å inngå avtale om lagerhold. Egne medarbeidere bør ha tilstrekkelig kompetanse for enkel feilsøking og -retting. Behov for assistanse må avtales med leverandør eller andre.

Krav til kompetanse for å installere utstyr i radioanlegg er regulert i lov om elektronisk kommunikasjon kommunikasjon (ekomloven) § 2-14, med tilhørende forskrifter; forskrift om elektroniske kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) kapittel 9, samt forskrift om autorisasjon for installatør av elektronisk kommunikasjonsnett og radioutstyr (autorisasjonsforskriften) kapittel 9.

[Lov om elektronisk kommunikasjon \(Ekomloven\)](#)

[Forskrift om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett \(autorisasjonsforskriften\)](#)



Krysskoplinger til andre paragrafer og regelverk

§ 2-10 Internkontroll

§ 4-7 Samband

§ 5-1 Sikringsplikt

Vedlegg til kap 5

Kapittel 6

Kapittel 7 dersom driftsradioen benyttes til driftskontrollfunksjoner

Enkeltvedtak Vedtak om beredskapsmessige kommunikasjonsmidler (2015, Unntatt offentlighet)

[Lov om elektronisk kommunikasjon \(Ekomloven\)](#)

§ 2-14

[Forskrift om autorisasjon for virksomhet som utfører installasjon og vedlikehold av elektronisk kommunikasjonsnett \(autorisasjonsforskriften\)](#) kapittel 9

Innhold

8. Avsluttende bestemmelser	1
8.1 Kontroll	1
8.2 Pålegg	3
8.3 Dispensasjon	3
8.4 Vedtak om tvangsmulkt	4
8.5 Vedtak om overtredelsesgebyr	5
8.6 Straff	7
8.7 Gebyr til beredskapsmyndigheten	7
8.8 Ikrafttreden	8
8.9 Forholdet til eldre vedtak om klassifisering og overgangsregler	8

8. Avsluttende bestemmelser

Formålet med bestemmelsene i dette kapitlet er at NVE ved kontroll og bruk av reaksjoner kan bidra til at kravene gitt i eller i medhold av kraftberedskapsforskriften blir overholdt. Les mer om NVEs tilsynsvirksomhet på <http://www.nve.no/tilsyn>.

Med *kontroll* menes kontrollerende aktiviteter med sikte på å undersøke etterlevelsen av gitte krav. Kontroll kan resultere i avvik eller anmerkning. *Reaksjoner* er handlinger og virkemidler som kan benyttes når avvik er avdekket. Hensikten med bruk av reaksjonsmidler er å sørge for effektiv etterlevelse av regelverket. Virkemidler i kraftberedskapsforskriften er bruk av tvangsmulkt, overtredelsesgebyr og straff.

8.1 Kontroll

§

§ 8-1. Kontroll

Beredskapsmyndigheten fører kontroll med at bestemmelser gitt i eller i medhold av denne forskriften overholdes.

Virksomheter skal medvirke til gjennomføring av kontroll. Dette omfatter blant annet å fremskaffe dokumentasjon og opplysninger som er nødvendige for å gjennomføre kontroll, og gi beredskapsmyndigheten adgang etter energiloven § 9-5 annet ledd.

Hva føres det kontroll med?

NVEs kontrollvirksomhet må ses i sammenheng med virksomhetenes plikt til internkontroll etter kbf § 2-10. Etter § 8-1 første ledd kan NVE føre kontroll med at

- bestemmelsene i kraftberedskapsforskriften overholdes
- vedtak truffet i medhold av kraftberedskapsforskriften overholdes

Hvem føres det kontroll med?

NVE kan kontrollere alle virksomheter forskriften gjelder for etter § 1-3. Dette omfatter

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

Hvordan fører NVE kontroll?

NVE (beredskapsmyndigheten) benytter følgende kontrollmetoder:

Revisjon	Revisjon er en uavhengig, systematisk og dokumentert gjennomgang hos virksomheten av anlegg, bygninger, systemer eller dokumenter
Inspeksjon	Inspeksjon er en uavhengig og dokumentert <i>fysisk kontroll</i> av anlegg og bygninger
Dokumentkontroll	Dokumentkontroll er å <i>innhente og gjennomgå dokumenter</i> (bilder og skriftlig materiale uansett lagringsmedium). Innhenting omfatter både innsendt informasjon og innhentet informasjon fra åpne kilder
Spørreundersøkelse	Spørreundersøkelse er en <i>skriftlig innhenting av informasjon</i> hos flere virksomheter samtidig gjennom et sett av likelydende spørsmål
Innrapportering	Kontroll av informasjon som fremkommer gjennom innrapporteringsordninger etter regelverk eller vedtak

NVE kan føre kontroll med virksomhetene i planleggings-, utbyggings-, drifts- og avviklingsfasen.

Kontrollen kan gjelde hele eller deler av virksomheten, og rette seg mot systemer, anlegg, virksomhetens interne prosedyrer, eller konkrete problemstillinger.

Kontroll kan være varslet eller uanmeldt. Kontroll kan utføres både på NVEs eget initiativ og på oppfordring fra andre.

Virksomhetenes medvirkningsplikt

Virksomhetene har plikt til å medvirke til at NVE kan gjennomføre tilsyn. Den særlige opplysningsplikten etter § 8-1 annet ledd suppleres av den generelle opplysningsplikten etter energiloven § 10-1 tredje ledd.

Medvirkningsplikten omfatter blant annet å fremskaffe dokumentasjon og opplysninger som er

nødvendige for å gjennomføre kontroll, og mot gyldig legitimasjon gi NVE adgang til grunn, bygg, anlegg og lignende, jf. energiloven § 9-5 annet ledd. NVEs interne adgangskort med bilde er gyldig legitimasjon. Det samme er HMS-kortet utstedt av Arbeidstilsynet. Kortene legitimerer at vedkommende har rett til adgang, men er ikke det samme som gyldig identifikasjon. For identifikasjon viser vi til blant annet til pass, nasjonalt ID-kort og førerkort.

8.2 Pålegg

§ 8-2. Pålegg

Beredskapsmyndigheten kan gi de pålegg som er nødvendige for gjennomføring av bestemmelser gitt i eller i medhold av denne forskrift.

Hva kan NVE gi pålegg om?

For at NVE skal kunne gi et pålegg, må det være nødvendig for gjennomføring av bestemmelser gitt i eller i medhold av kraftberedskapsforskriften.

Pålegg kan for eksempel være pålegg om retting. Et vedtak med pålegg om retting omfatter alt virksomheten blir pålagt å gjennomføre for at virksomhetens systemer eller anlegg skal bli i tråd med regelverket.

NVE kan gi pålegg om retting i tilfeller hvor det er mulig å gjøre tiltak som sørger for lovlig tilstand. Retting er for eksempel aktuelt der et klassifisert anlegg ikke oppfyller kravene til fysisk sikring, eller der beredskapsplanen ikke oppfyller kravene i forskriften.

NVE setter en frist for retting. Fristen settes slik at virksomheten har en reell mulighet til å rette på forholdet innen fristen. NVE vil ta hensyn til årstiden og til praktiske forhold, som for eksempel leveringstid på anleggsdeler.

8.3 Dispensasjon

§ 8-3. Dispensasjon

Beredskapsmyndigheten kan i særlige tilfeller gi dispensasjon fra bestemmelser gitt i eller i medhold av denne forskrift.

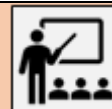
Denne bestemmelsen gir NVE hjemmel til å gi dispensasjon fra bestemmelser gitt i eller i medhold av forskriften. En slik dispensasjon gis ved enkeltvedtak.

Når kan dispensasjon gis?

For å gi dispensasjon fra bestemmelser i kraftberedskapsforskriften eller fra enkeltvedtak gitt i medhold av denne, må det foreligge et *særlig tilfelle*.

At bestemmelsen stiller krav om at det foreligger et *særlig tilfelle*, innebærer at det skal mye til før NVE kan gi dispensasjon. Hva som er *særlig tilfelle*, må vurderes konkret i hver enkelt sak. Med et særlig tilfelle menes forhold som er vesentlig avvikende fra det som er vanlig i norsk kraftforsyning. Økonomiske og miljømessige forhold vil i svært liten grad gi grunnlag for dispensasjon. Bestemmelsen blir praktisert strengt.

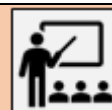
NVE kan sette vilkår for en dispensasjon.



Eksempel: Ønske om felles IKT-sikkerhetskoordinator

NVE mottok søknad om dispensasjon fra § 2-2 som pålegger KBO-enhetene å utpeke funksjonene beredskapsleder, beredskapskoordinator og IKT-sikkerhetskoordinator. Søknaden var begrunnet i et ønske om at flere KBO-enheten kunne dele en ekstern ressurs som dekket funksjonen IKT-sikkerhetskoordinator. Denne funksjonen inngår i kjernevirksomheten (beredskap) og er derfor ikke noe KBO-enhetene kan tjenestestutsette. NVE har godtatt at funksjonene etter § 2-2 kan deles i et konsern uten at det er nødvendig å søke om dispensasjon.

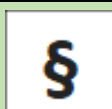
NVEs avsto søknaden. Begrunnelsen for avslaget var at det ikke forelå et særlig tilfelle som ga grunnlag for dispensasjon.



Eksempel: Utøvelse av driftskontrollfunksjoner under en pandemi

Dersom driftskontrollfunksjoner i klasse 3 må løses hjemmefra på grunn av sykdom eller strenge karantenebestemmelser under en pandemi, kan dette anses som et særlig tilfelle som kan gi grunnlag for dispensasjon. Søknad må sendes til NVE.

8.4 Vedtak om tvangsmulkt



§ 8-4. Tvangsmulkt

Ved overtredelse av bestemmelser gitt i eller i medhold av denne forskrift, kan beredskapsmyndigheten ilegge tvangsmulkt i medhold av energiloven § 10-3.

Ordforklaring

Tvangsmulkt	Dersom en ulovlig situasjon ikke opphører innen en fastsatt frist, kan NVE treffe vedtak om at det vil påløpe et offentlig pengekrav mot overtreder. Denne type pengekrav kalles tvangsmulkt. Tvangsmulkten virker fremover i tid, og har som formål å tjene som et oppfylleelsespress for å gjenopprette lovlig tilstand eller etterlevelse av pålegg. Tvangsmulkt kan fastsettes enten som en løpende mulkt eller som et engangsbeløp.
-------------	--

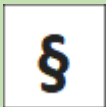
Forskriften gir NVE hjemmel til å bruke tvangsmulkt som reaksjon. Henvisningen til *energiloven* § 10-3 betyr at bruken av tvangsmulkt må skje innenfor rammene av denne bestemmelsen.

Etter energiloven § 10-3 kan det fastsettes en tvangsmulkt som enten løper inntil forholdet er bragt i orden, for eksempel dagmulkt, eller som et engangsbeløp pr. inntrådt overtredelse. Det kan fastsettes en bestemt frist for gjennomføringen av pålegg og en daglig løpende tvangsmulkt til statskassen dersom fristen oversittes. Blir pålegget ikke oppfylt innen den fastsatte fristen, kan departementet gjennomføre pålegget på vedkommende bekostning. Tvangsmulkt og utgifter til gjennomføring av pålegg, er tvangsgrunnlag for utlegg.

Når bruker NVE tvangsmulkt?

NVE bruker tvangsmulkt når plikter som er gitt i eller i medhold av denne forskriften, ikke blir oppfylt, og pålegg om retting av disse ikke er gjennomført innen den fastsatte fristen. Dette kan for eksempel være dersom avvik etter tilsyn ikke blir lukket innen rettefristen. Bruk av tvangsmulkt varsles av NVE.

8.5 Vedtak om overtredelsesgebyr



§ 8-5. Overtredelsesgebyr

Ved overtredelse av bestemmelsene i kapittel 2 til 7, inkludert vedleggene til kapittel 5, og vedtak truffet i medhold av § 8-3 kan det ilegges overtredelsesgebyr i medhold av energiloven § 10-7.

Bestemmelsen gir NVE hjemmel til å bruke overtredelsesgebyr som reaksjon. Henvisningen til energiloven § 10-7 betyr at bruken av tvangsmulkt må skje på de vilkår som følger av denne bestemmelsen.

Ordforklaring

Overtredelsesgebyr	Et overtredelsesgebyr innebærer at NVE pålegger en virksomhet å betale et pengebeløp til det offentlige som følge av at virksomheten har brutt et forbud eller påbud som er fastsatt i lov, forskrift eller enkeltvedtak. Overtredelsesgebyr er en administrativ sanksjon som skiller seg fra straff ved at det er forvaltningen (NVE) og ikke domstolene/politiet som ilegger reaksjonen.
---------------------------	--

Når bruker NVE overtredelsesgebyr?

Overtredelsesgebyr er en sanksjon som kan benyttes mot brudd på de bestemmelsene i kraftberedskapsforskriften som er særskilt nevnt i § 8-5. I tillegg er det adgang til å ilegge overtredelsesgebyr for brudd på *energiloven* kapittel 9.

For å treffe vedtak om å ilegge overtredelsesgebyr, må følgende være oppfylt

- handlingen eller unnlatelsen må rent objektivt rammes av krav som angitt i § 8-5
- det må foreligge subjektiv skyld, enten i form av forsett eller uaktsomhet
- NVE mener overtredelsesgebyr bør ilegges basert på en skjønnsmessig vurdering

På energilovens område vil de fleste overtredelser begås av virksomheter. For at en virksomhet skal kunne ilegges overtredelsesgebyr, må det også foreligge skyld, enten i form av forsett eller uaktsomhet, hos enkeltperson(er) som handler på vegne av virksomheten. Virksomheten er ansvarlig for feil der det er ukjent hvem som er ansvarlig for feilen. Virksomheten er også ansvarlig for feil som oppstår på grunn av flere enkelthendelser som hver for seg ikke medfører havari eller avbrudd.

For uhell og særlige omstendigheter som ikke er under menneskelig kontroll, som for eksempel naturkatastrofer, kan ikke virksomheten ilegges overtredelsesgebyr.

Ved avgjørelsen av om overtredelsesgebyr skal ilegges og ved utmåling av sanksjonen, skal det etter energiloven § 10-7 særlig legges vekt på

- a) overtredelsens grovhet
- b) om overtreder ved retningslinjer, instruksjon, opplæring, kontroll eller andre tiltak kunne forebygget overtredelsen
- c) om overtredelsen er begått for å fremme overtrederes interesser
- d) om overtreder har hatt eller kunne oppnådd noen fordel ved overtredelsen
- e) om det foreligger gjentakelse
- f) overtrederes økonomiske evne

8.6 Straff



§ 8-6. Straff

Overtredelse av bestemmelsene i kapittel 2-8, inkludert vedleggene til kapittel 5, kan straffes med bøter eller fengsel i medhold av energiloven § 10-5.

Ordforklaring

Straff	Med straff menes bøter eller fengsel. Energiloven § 10-5 har ulike strafferamme for forsettlig og uaktsomme overtredelser: • Forsettlig overtredelse kan straffes med bøter eller fengsel i inntil 1 år eller begge deler • Uaktsomme overtredelser kan straffes med bøter eller fengsel i inntil 3 måneder eller begge deler
---------------	---

Kraftberedskapsforskriften § 8-6 bør ses i sammenheng med § 8-5 om overtredelsesgebyr, som gir forvaltningen flere alternative sanksjonsmuligheter. Straff kan kun benyttes mot brudd på de bestemmelsene i kraftberedskapsforskriften som er angitt i § 8-6. Videre kan brudd på energiloven straffes.

Hvem kan ilegge straff?

Verken kraftberedskapsforskriften eller energiloven gir NVE hjemmel til å straffe med fengsel eller bøter. Dersom NVE vurderer at noen som har gjort noe straffbart etter kraftberedskapsforskriften eller kapittel 9 i energiloven bør ilegges straff, må saken anmeldes til politiet. Domstolene ilegger eventuelt straff.

8.7 Gebyr til beredskapsmyndigheten



§ 8-7. Gebyr til beredskapsmyndigheten

Til dekning av beredskapsmyndighetens utgifter til arbeidet med kraftforsyningsberedskap innkreves et årlig gebyr.

Gebyret fastsettes for den enkelte KBO-enhet på grunnlag av installert ytelse i klassifiserte anlegg og nettstasjoner pr. 1. januar det år gebyret beregnes for. Satsene skal reguleres slik at de samlede gebyrer tilsvarer de faktiske utgifter beredskapsmyndigheten har med beredskapsarbeidet.

NVE krever inn gebyr med hjemmel i *energiloven* § 9-6 for å finansiere utgifter til beredskapsarbeidet i kraftforsyningen. Utgiftene utlignes på eiere og brukere av de anlegg kapittel 9 i loven omfatter. Det forekommer at eier og bruker ikke er samme virksomhet. NVE sender regning for beredskapsgebyr til den KBO-enheten som er *bruker* av det klassifiserte anlegget. Les mer her:

<https://www.nve.no/damsikkerhet-og-kraftforsyningsberedskap/kraftforsyningsberedskap/>

8.8 Ikrafttreden

§

§ 8-8 Ikrafttreden

Denne forskriften trer i kraft 1. januar 2013. Fra samme tid oppheves forskrift 16. desember 2002 nr. 1606 om beredskap i kraftforsyningen.

8.9 Forholdet til eldre vedtak om klassifisering og overgangsregler

§

§ 8-9. Forholdet til eldre vedtak om klassifisering og overgangsregler

Kraftstasjoner klassifisert i klasse 1 med installert ytelse under 50 MVA, er ikke lenger klassifisert. Fjernvarmesentraler klassifisert i klasse 1 ved enkeltvedtak og som har lavere installert ytelse enn 50 MW, er ikke lenger klassifisert.

Øvrige vedtak om sikring eller andre vedtak i medhold av forskrift 16. desember 2002 nr. 1606 om beredskap i kraftforsyningen truffet etter 1. januar 2003 og før 1. januar 2013 står fortsatt ved lag inntil de blir endret eller opphevet i medhold av denne forskrift.

Anlegg som er idriftssatt før 1. januar 2013, og som ikke er omfattet av vedtak omtalt i annet ledd, klassifiseres etter denne forskrift, men slik at sikringstiltak etter kapittel 5 kan tilpasses bygningsteknisk utforming og tidligere pålegg om fysisk sikring. Ved vesentlig ombygging eller utvidelse vil kravene etter kapittel 5 gjelde fullt ut for den del av anlegget som endres.

Vedtak om beredskapsmessige forhold til kraftforsyningen om annet enn klassifisering og sikringstiltak truffet før 1. januar 2003, og som ikke er erstattet av senere vedtak eller forskrifter står ved lag så langt de passer inntil de blir endret eller opphevet i medhold av denne forskrift.

Alle anlegg som er satt i drift etter 1. januar 2013 skal klassifiseres og sikres etter denne forskrift. Dette gjelder selv om de har fått konsesjon før 2013. For disse anleggene gjelder en overgangsperiode på 2 år. Beredskapsmyndigheten kan gi én dispensasjon fra dette. Slik dispensasjon kan kun gis én gang for hvert anlegg for en periode på inntil 2 år.

Bestemmelsen beskriver forholdet mellom dagens forskrift og tidligere regelverk og vedtak. Etter *energilooven* kapittel 9 kan NVE stille krav om å gjennomføre nye eller endrede tiltak ved både nye og eksisterende kraftforsyningsanlegg, uavhengig av tidligere pålegg.

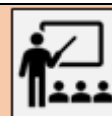
Første ledd forskriftsfester at kraftstasjoner med mindre installert ytelse enn 50 MVA som tidligere var klassifisert i klasse 1, ikke lenger er det. Det samme gjelder for tidligere klassifiserte fjernvarmeanlegg under 50 MW. Den tidligere klassifiseringsgrensen var 25 MVA for kraftstasjoner. Mange fjernvarmeanlegg på minst 10 MJ/s var klassifisert ved enkeltvedtak før 2013.

Nærmere om forholdet til beredskapsforskriften fra 2002

Annet ledd angir at vedtak om sikring truffet etter beredskapsforskriften fra 2002 (BfK) fremdeles gjelder. Annet ledd omfatter *ikke* vedtak om klassifisering og sikring som er truffet før BfK trådte i kraft 1. januar 2003.

Også andre vedtak truffet etter BfK gjelder frem til de blir opphevet av NVE.

Formuleringen ”inntil de blir endret eller opphevet” er en henvisning til § 5-7 og adgangen til å fatte enkeltvedtak om klassifisering og sikringstiltak.



Eksempel: anlegg bygget og klassifisert før 2003

Tangefjord kraftverk med 55 MVA installert ytelse ble satt i drift i 1976. Anleggets betydning for kraftforsyningen ble vurdert til å være høy, spesielt for lokal forsyning på grunn av dårlig nettkapasitet i området. Anlegget ble klassifisert i høyeste klasse som den gang var klasse 1; nå klasse 3. Etter som tiden har gått, har det kommet til flere kraftstasjoner i området og nettet er forsterket. Tangefjord kraftverk har ikke lenger samme betydning. Enkeltvedtaket om klasse var fra 1972. Det gamle vedtaket er ikke lenger gyldig av to grunner. Vedtaket var ikke gitt med hjemmel i BfK i perioden 1. januar 2003 til 1. januar 2013 og anlegget ble satt i drift før 1. januar 2013. Det blir derfor klassifisert etter kbf (denne forskriften) uten at NVE skriver et nytt enkeltvedtak. Kraftverket kommer i klasse 1 fordi det er på minst 50 MVA og under 100 MVA.



Eksempel: anlegg bygget og klassifisert mellom 2003 og 2013

Sjukehuset varmesentral har to oljekjeler og en elektrokjel på til sammen med 75 MW. Varmesentralen ble satt i drift i 2008. Sentralen ble vurdert å være svært viktig for sjukehuset. Varmesentralen ble klassifisert i høyeste klasse for fjernvarmeanlegg; det vil si klasse 2. Enkeltvedtaket om klasse var fra 2009. Vedtaket er gyldig fordi det er gitt med hjemmel i BfK i perioden 1. januar 2003 til 1. januar 2013. Hadde det blitt klassifisert etter kbf (denne forskriften) ville det kommet i klasse 1 fordi det er på minst 50 MW og under 150 MW.



Eksempel: anlegg bygget og klassifisert mellom 2003 og 2013

Østre transformatorstasjon har to transformatorer på 20 MVA, til sammen 40 MVA. Transformatorstasjonen ble satt i drift i 2012 og NVE klassifiserte den med et enkeltvedtak til å være i klasse 2 i 2010. Vedtaket er gyldig fordi det er gitt med hjemmel i BfK i perioden 1. januar 2003 til 1. januar 2013. Hadde det blitt klassifisert etter kbf (denne forskriften) ville det kommet i klasse 1 fordi det er på minst 10 MVA og under 50 MVA.

Anlegg uten enkeltvedtak etter beredskapsforskriften fra 2002

Tredje ledd omhandler eldre anlegg som ikke er omfattet av enkeltvedtak etter beredskapsforskriften av 2002 i perioden 01.01.2003 til 01.01.2013.

Reglene om sikring og klassifisering etter kbf med presiseringene nedenfor, gjelder uavhengig av om det er truffet vedtak om sikring og klassifisering i medhold av beredskapsforskriften av 2002 eller ikke. Mange eksisterende anlegg vil være av eldre dato, noe anleggene kan bære preg av. NVE forventer at mange eldre anlegg vil utvides eller ombygges i årene framover. På grunn av anleggets utforming vil det i mange tilfeller ikke være hensiktsmessig å gjennomføre sikringstiltak som helt ut fyller krav etter denne forskriften for eksisterende anlegg.

Overgangsbestemmelsen innebærer at det kan tas hensyn til anleggenes alder og i hvilken grad de oppfyller tidligere pålagte sikringstiltak ved vurderingen av om et anlegg oppfyller krav til sikring. Utgangspunktet er likevel at tidligere pålagte sikringstiltak er gjennomført. Dette gjelder selv om disse ikke er hensiktsmessige etter dagens forhold, eller at de ikke fullt ut oppfyller dagens forskrift.

Normalt krever ikke NVE at det skal utføres sikringstiltak som innebærer vesentlige endringer i planløsninger, bygningsmasse eller hvordan de elektriske høyspenningsanleggene er arrangert, og som medfører store ombygginger av eksisterende anlegg. Dette gjelder likevel ikke særlig viktige anlegg eller særlig dårlig sikrede anlegg.

Tredje ledd gir ikke grunnlag for dispensasjon fra tidligere pålagte tiltak som ikke er gjennomført.



Eksempel: Transformatorstasjon med enkel kabelføring

Ved tilsyn i en transformatorstasjon i klasse 3 ble det oppdaget at kabler for styring og samband, nød- og stasjonsstrøm og høyspent alle lå i samme kabelføring. Stasjonen var bygget på 70-tallet etter datidens krav til sikring. En omlegging og fysisk separering ville kreve større bygningsmessige endringer. NVE besluttet derfor at kravet om dubberte og fysisk uavhengige kabelføringer skulle utstå til stasjonen eventuelt skulle bygges om.

Eldre vedtak om tilskudd til reservemateriell

Fjerde ledd viser også til vedtak som tidligere er truffet om tilskudd til og forvaltning av reservemateriell, og innebærer at vilkårene om forvaltning av reservemateriellet fremdeles gjelder. Dette er nærmere behandlet i kapittel fire. Bestemmelsen gjelder også eventuelle andre vedtak.

VEILEDNING KRAFTBEREDSKAPSFORSKRIFTEN:

SIKRINGSTILTAK FOR KLASSIFISERTE ANLEGG, kbf § 5-4 vedlegg 1, §5-5 vedlegg 2, §5-6 vedlegg 3 og vedlegg 4



Innholdsfortegnelse

1	VEDLEGG 1: KRAV TIL ANLEGG I KLASSE 1.....	5
1.1	Transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg	5
1.2	Driftskontrollsystemer	7
1.3	Kraftledninger	9
2	VEDLEGG 2 OG 3: FUNKSJONSBASERTE KRAV KLASSE 2 OG 3.....	10
3	VEDLEGG 2 OG 3: SPESIFIKKE KRAV FOR STASJONER KL.2 OG 3:.....	11
3.1	Oppdagelse av uønskede hendelser og handlinger	12
3.2	Fysisk beskyttelse av anlegg	14
3.3	Redundans	19
3.4	Stasjonsstrøm og nødstrømsanlegg	20
3.5	Geomagnetisk induerte strømmer	24
4	VEDLEGG 2 OG 3: TILLEGG FOR KRAFTSTASJONER, KL. 2 OG 3	25
4.1	Kraftstasjoner bygget i fjell.....	25
4.2	Kraftstasjoner bygget i dagen.....	29
4.3	Overvåkning, brannsikring og sonesikring i kraftstasjon.....	30
4.4	Redundans, stasjonsstrøm og nødstrøm i kraftstasjon.....	31
4.5	Oppstart av kraftstasjon på spenningsløst nett	32
5	VEDLEGG 2 OG 3: - TILLEGG FOR DRIFTSKONTROLLSYSTEMER, KL. 2 OG 3	33
5.1	Driftssentraler	33
5.2	Sambandsanlegg.....	37
6	VEDLEGG 2 OG 3: KRAFTLEDNINGER KL. 2 OG 3	39
7	VEDLEGG 2: FJERNVARMEANLEGG, KL. 2	40
8	VEDLEGG 4 NORMER OG STANDARDER	41
8.1	Relevante normer og standarder	41
8.2	Sammenhengen mellom sikringsnivå i kbf og sikringklasser i utvalgte europeiske standarder	43
9	TILLEGG OM BEREDSKAPSRUM	44
9.1	Drift og vedlikehold	44
9.2	Kontroll	44
9.3	Eksisterende beredskapsrom	45
9.4	Beredskapsrom – utstyr, drift, vedlikehold og kontroll.....	46
10	REFERANSER	47

Ordforklaring

Redundans	Reservekapasitet/dublering av kritiske komponenter og funksjoner for å øke påliteligheten til systemet										
Stasjonsstrøm	Stasjonens strømforsyning for egen drift og sikkerhet – styring, overvåkning, vern, lys og stikk, og øvrige hjelpeanlegg (VVS, pumper, kompressorer m.v.), inkludert nødstrømsforsyning dersom ordinær strømforsyning svikter.										
Nødstrøm	Reserveløsning for strømforsyning ved bortfall av ordinær stasjonsstrøm, i form av stasjonært aggregat, mobilt aggregat eller begge deler. Må kombineres med batteribank(er) for å kunne oppnå avbruddsfri strømforsyning.										
Kontrollutrustning	Utrustning i lokale og sentrale kontrollanlegg for å overvåke tilstand og styre brytere i kraftforsyningen.										
Styresignaler	Signaler som formidles elektronisk (automatiske eller manuelle) over kommunikasjonsnett fra kontrollutrustningen.										
HB	Hardhet Brinell: Brinellhardhet er et mål på hardheten til metaller og legeringer. Ved brinellhardhetstesting trykkes en hard kule med diameter 10 mm mot en plan flate med en valgt last. Diameteren på inntrykket måles, og et hardhetsnummer, HB, bestemmes ut fra en kalibrert skala. Brinellhardheten angis som forholdet mellom presskraften og arealet av den sirkelen som dannes i materialflaten. (kilde: Store norske leksikon)										
FG-klasse	Regler for lås og beslag utgitt av Forsikringsselskapenes Godkjenningsnevnd										
Brannklasse	Ut fra den konsekvensen en brann kan innebære for skade på liv, helse, samfunnsmessige interesser og miljøet, skal byggverk eller ulike deler av et byggverk plasseres i brannklasser etter tabellen nedenfor. Brannklassene skal legges til grunn for prosjekteringen og utførelsen for å sikre byggverkets bæreevne mv. ved brann. <table data-bbox="737 1505 1235 1807"> <tr> <th>Brannklasse</th><th>Konsekvens</th></tr> <tr> <td>1</td><td>Liten</td></tr> <tr> <td>2</td><td>Middels</td></tr> <tr> <td>3</td><td>Stor</td></tr> <tr> <td>4</td><td>Særlig stor</td></tr> </table> (kilde: § 11-3 i Tek 17))	Brannklasse	Konsekvens	1	Liten	2	Middels	3	Stor	4	Særlig stor
Brannklasse	Konsekvens										
1	Liten										
2	Middels										
3	Stor										
4	Særlig stor										
Brannmotstand	En konstruksjons evne til i en gitt tid å opprettholde bæreevne, stabilitet, integritet og varmeisolering slik at den tilfredsstiller angitte krav ved standardisert brannprøving. (kilde: Kollegiet for brannfaglig terminologi)										

<i>REI M</i>	I dag følges Euroklassesystemet, hvor brannmotstanden til bygningsdeler og konstruksjoner deles inn etter følgende fire kriterier med tilhørende bokstavkoder: bæreevne – R integritet – E isolasjonsevne – I mekanisk motstandsevne – M Bokstavkoden etterfølges av motstandstiden i minutter: 15, 30, 60, 90 og så videre. (<i>kilde: Store norske leksikon</i>)
<i>HF-sperre</i>	Induktans (luftspole) som sperrer for høyfrekvente signaler i luftledninger ved overgang mellom luftledning og stasjonsanlegg. Signalene ledes frem til kontrollanlegget gjennom en kapasitiv kobling med spenningsdeling (høyspenningskondensator).  © 2021 Trench Group

1 VEDLEGG 1: KRAV TIL ANLEGG I KLASSE 1

1.1 Transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg

klasse 1
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 1.1 til 1.3</i>
Fysisk sikring, adgangskontroll og brannmotstand
1.1 For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og fjernvarmeanlegg gjelder følgende krav:
1.1.1 Det skal etableres en adgangskontrollert sone som omfatter alle adkomster til anlegget. Fysisk sikring skal som et minimum omfatte et solid bygg med dører/ porter, vinduer og øvrige adkomster. Disse skal oppfylle krav til normalt sikringsnivå etter fastsatte normer.
Alle installasjoner skal ha fysisk beskyttelse. I friluftsanlegg kan dette være et flettverksgjerde med låst port. Innendørsanlegg skal ha fysisk beskyttelse (skallsikring), minimum i form av et låsbart lettbygg (elementer, plater eller liknende).
Alle utvendige dører, porter og andre mulige adkomster bør sikres etter sikkerhetsklasse 3 etter gjeldende EN-normer og tilsvarende låseanordninger i FG (Forsikringsselskapenes godkjenningnemnd) klasse 2 eller bedre. Hærverkshemmende vinduer i klasse P4A eller P5A etter EN 356 (se veiledning til vedlegg 4), eller andre måter å beskytte vinduer og andre mulige adkomster på.
1.1.2 Brannsikring skal oppfylle krav i henhold til andre relevante forskrifter og normal brannmotstand etter fastsatt norm.
Brannsikring etter veiledningen til <i>forskrift om elektriske forsyningsanlegg</i> (fef) § 4-9 Sikkerhetstiltak og sikkerhetsutstyr, eller bedre. Man skal vurdere å innføre tilleggssikring i forhold til egne akseptkriterier og ut fra analyse av anleggets betydning og lokal risiko, se også §§ 5-3 og 5-8. Dette kan eksempelvis være tiltak som gjelder for grunnsikring transformatorstasjon klasse 2.
1.1.3 Rom for lokal driftskontroll, styring og samband skal være egne adgangskontrollerte soner, og skal oppfylle krav til normalt sikringsnivå og brannmotstand etter fastsatte normer.
Se veiledningen til krav 1.1.1



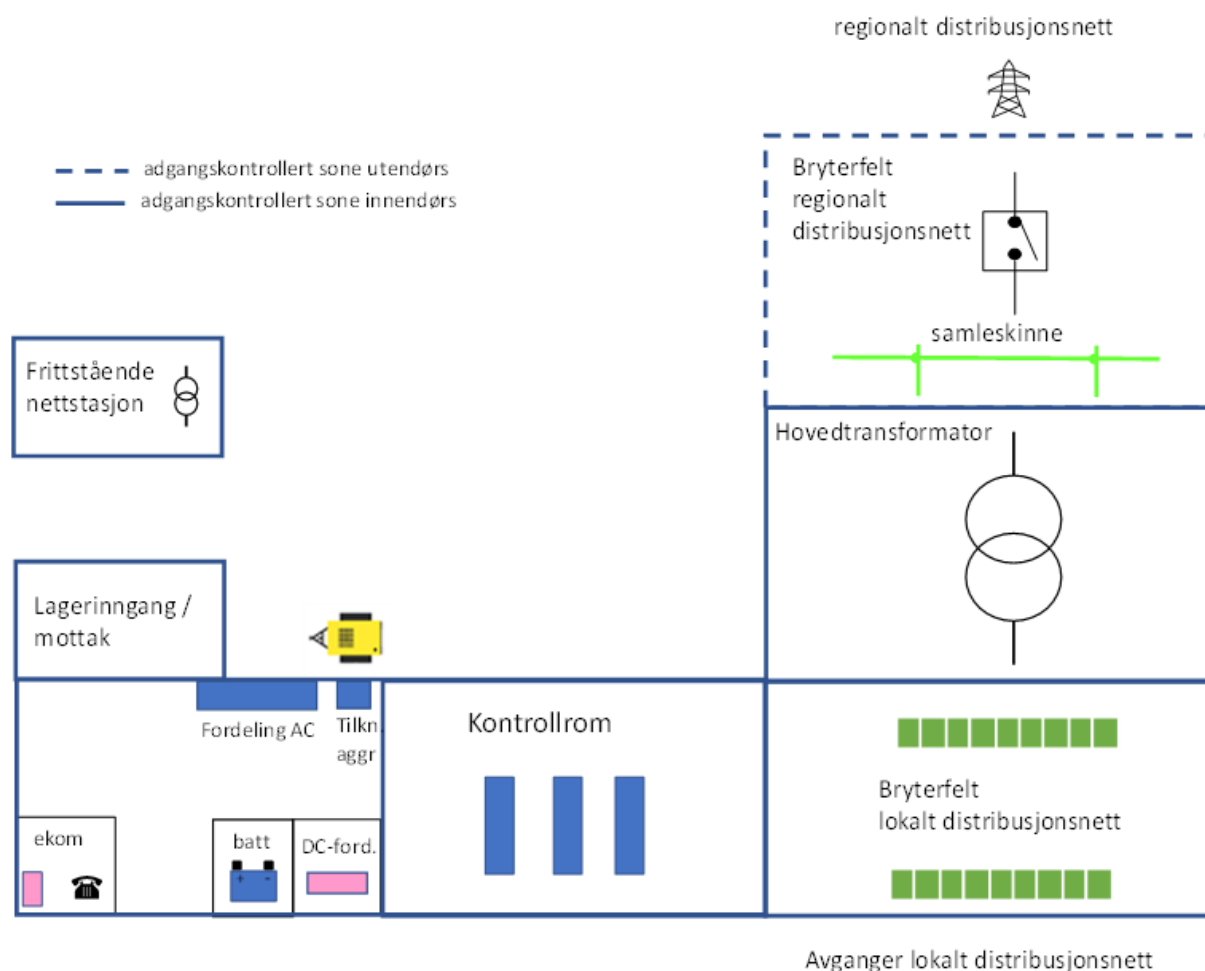
Eksempel: Sikringsnivå i kraftbereskapsforskriften vs forskrift om elektriske forsyningsanlegg (fef)

Det er gjennomført flere prosjekter for å finne om det er motstridende krav eller alvorlige hull i kravene gitt i hhv kbf og fef:

- Regelverksprosjektet mellom NVE, DSB og Statnett (NVE Rapport 2/2009)
- Sikker levering av elektrisk energi – Grensesnittet mellom DSB og NVE (Difi Rapport 4/2009)
- Overlappprosjektet mellom NVE og DSB

Konklusjonen var at det ikke finnes motstridende krav eller vesentlig hull. Fef angir et grunnnivå og kbf tilleggskrav.

Figur 1 viser prinsippskisse for klasse 1 stasjonsanlegg



Figur 1: Prinsippskisse for klasse 1 stasjonsanlegg

Nødstrøm og reserver
1.1.4 For egen stasjonsstrømforsyning skal anlegget ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Et mobilt aggregat må kunne kobles til innenfor batteritiden. Anlegget må samlet sett ha en gangtid på minst ett døgn.
Samlet skal batterianlegg og nødstrømsaggregat gi en strømforsyning uten avbrudd i minst ett døgn. Nødstrømsanlegget må ha kapasitet til å opprettholde anleggets viktigste funksjoner. Virksomheten må forberede tilkobling av nødstrømsaggregat, og aggregatet må alltid være så tilgjengelig at det faktisk kan kobles til før batteriene tar slutt. Utholdenhet vil blant annet være avhengig av at det etableres rutiner for etterfylling av drivstoff og annet vedlikehold. Utover dette må den som eier selv vurdere kapasitet og utholdenhet ut fra anleggets art og betydning, samt sannsynligheten for utfall i ordinær strømforsyning og konsekvenser av dette. På utsatte steder og hvor ekstraordinære forhold kan gi langvarige utfall må lenger utholdenhet vurderes. For driftssentraler skal de systemene som har betydning for driften av kraftsystemet, forsynes fra batterianlegg/UPS (Uninterruptible Power Supply) som bør ha en driftstid på minst 2 timer. Et mobilt nødstrømsaggregat må uansett kunne kobles til innen den driftstid batterianlegget gir. Dersom driftssentralen er lokalisert sammen med KBO-enhetens administrasjon og ledelse bør permanent nødstrømsaggregat vurderes. Sambandsanleggene bør utstyres med batterianlegg med driftstid ½ -1 døgn eller mer, avhengig av tilgjengelighet. Det bør uansett planlegges og forberedes tilkobling av nødstrømsaggregat.
1.1.5 Det skal være tilgang på reserver for viktige komponenter.
Det er ikke spesifikke krav til redundans for anlegg i klasse 1, men viktige komponenter skal kunne erstattes. Se § 4-4 (materiell og utstyr). Behovet for redundans og tilgang på reservemateriell må avgjøres gjennom risikovurdering.
Tilleggsveiledning for fjernvarme
Fjernvarmesentraler skal sikres som øvrige produksjonsanlegg i klasse 1, så langt disse reglene passer. NVE har utarbeidet en egen veiledning om fjernvarmeberedskap, se NVE veileder nr. 5-2015.

1.2 Driftskontrollsystemer

klasse 1
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 1.1 til 1.3</i>
1.2 For driftskontrollsystemer gjelder følgende krav:
Driftssentraler
1.2.1 Driftssentraler
1.2.1.1 Driftssentraler skal plasseres i et bygg med normal brann- og innbruddssikkerhet.
Rom for driftssentral skal utføres som branncelle(r) (mot tilstøtende rom, også over og under) med en brannmotstand på minst EI 30 (selvluukkende dører bør vurderes). Tilsvarende brannsikring for kabelgjennomføringer med mer.

Nødvendige slukkemidler for å slå ned en mindre brann raskt, må være tilgjengelig. Rommet må være låst med FG godkjent lås.
1.2.1.2 Skal ha et effektivt innbrudds- og brannvarslingssystem.
Driftssentralen skal ha brann- og innbruddsalarm med effektiv varsling av hjemmevakt, lokalt brannvesen eller annen bemannet driftssentral, installert for driftssentralen.
1.2.1.3 Skal være normalt fysisk sikret etter fastsatt norm.
Rom for driftssentral skal utføres med solide låsbare dører som sammen med annen sikring av adkomster bør oppfylle sikkerhetsklasse 3 (enkel innbruddsikring) etter EN. Operatørrom bør ha hærverkshemmende vinduer etter EN 356. For øvrige (tekniske) rom unngås vinduer.
1.2.1.4 Skal være utstyrt med avbruddsfri strømforsyning og mulighet for tilkobling av mobilt nødstrømsaggregat, med en samlet gangtid på minst ett døgn.
Se veiledningen til krav 1.1.4
1.2.1.5 Skal ha et alternativt opplegg for utøvelse av viktige funksjoner for drift og ledelse i en ekstraordinær situasjon.
<i>Alternativt opplegg:</i> Driftskontrollsystemer i klasse 1 skal ut fra sin funksjon og betydning ha et alternativt opplegg for drift, ledelse og gjenoppretting i ekstraordinære situasjoner. Se også § 7-8. Det skal fungere dersom den ordinære driftssentralen havarer, må evakueres eller blir ødelagt av for eksempel brann. Ved alternativ drift skal viktige funksjoner kunne ivaretas på en sikker og effektiv måte. Det kan gjøres ved hjelp av et forberedt alternativt sted eller ved lokal betjening av aktuelle anlegg. Det er opp til den enkelte enheten å planlegge og etablere slik alternativ drift. Sambandsopplegget må være klart, og øvelser må gjennomføres, blant annet for å kontrollere at opplegget virker og for å etablere og opprettholde kompetansen i forhold til en alternativ drift.
Sambandsanlegg
1.2.2 For sambandsanlegg gjelder følgende krav:
1.2.2.1 Sambandsanlegg regnes normalt som en del av det driftskontrollsystem de betjener og skal planlegges og utføres etter de påregnelige påkjenninger de kan bli utsatt for.
<i>Ytre påkjenninger:</i> Sambandsanlegg skal planlegges og utføres etter de maksimalbelastningene (uvær, ising med videre) de kan bli utsatt for. Dette gjelder særlig utsatte komponenter med tilhørende oppheng/føringer og festeanordninger som kabler, master, antenner, radiospeil, HFsperrer med mer.
1.2.2.2 Anlegget skal sikres mot uønskede hendelser og handlinger som innbrudd, hærverk, sabotasje og brann.
<i>Sikring mot uønsket adgang og brann:</i> Sambandsanlegg skal gis en tilfredsstillende fysisk sikring etter klasse og risiko for inntrenging, sabotasje, brann og andre former for ødeleggelse. Dette kan gjøres eksempelvis ved bruk av ikke brennbare materialer, brannslukkingsanlegg/-utstyr, brann- og innbruddsalarm. Vinduer skal unngås i alle anlegg, eventuelt skal de sikres med hærverks- eller innbruddshemmende glass, stållemmer, solide gitter eller liknende som låses eller boltes fra innsiden. Antenneanlegg, master og kabelføringer sikres mot hærverk, sabotasje, uønsket adgang og brann.

Dette omfatter tiltak som bruk av ikke brennbare materialer, beskyttelse av kabler, inngjerding av master og tildekking/beskyttelse av kabeltrasé fram til disse. Strømforsyning og samband bør føres inn i anlegget gjennom jordkabler eller gis annen beskyttelse. Master beskyttes med klatrehindre.
<i>1.2.2.3 Anlegget skal utstyres med nødstrøm med automatisk start og gangtid på minst ett døgn.</i>
Se veiledningen til krav 1.1.4
<i>1.2.2.4 Anlegget skal også oppfylle kravene som fremgår av § 4-7.</i>
Se veiledningen til § 4-7 (samband)

1.3 Kraftledninger

klasse 1
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 1.1 til 1.3</i>
1.3 For kraftledninger gjelder følgende krav
1.3.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessige betydning.
En risikovurdering bør ta hensyn til stedlige forhold som for eksempel adkomst og tilgjengelighet for linjerydding og feilretting mv. Risikovurderingen bør også ta hensyn til klimavariasjoner og ev. økt fare for naturgitte hendelser på grunn av klimaendringer. Kraftledningenes samfunnsmessige betydning kan f.eks. være kraftforsyning til helseinstitusjoner, offentlig beredskapsvirksomhet, mv. i henhold til egen oversikt over prioriterte kunder som virksomheten skal ha utarbeidet i en beredskaps- eller rasjoneringsplan etter § 6a og vedlegg 1 i <i>krafttrasjoneringsforskriften</i> .

2 VEDLEGG 2 OG 3: FUNKSJONSBASERTE KRAV KLASSE 2 OG 3

<i>klasse 2</i>	<i>klasse 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Funksjonsbaserte krav	
2.1. For transformatorstasjoner, koblingsstasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav: 2.1.1 Anleggets sikringsnivå skal ivaretas gjennom en kombinasjon av blant annet følgende tiltak: a. Uønskede hendelser og handlinger skal oppdages raskt og håndteres av et effektivt reaksjonsmønster. b. Fysisk og elektrisk utførelse og beskyttelse skal være på et nivå som begrenser tap av funksjon og ødeleggelse. c. Gjenoppretting av eventuelle funksjonstap skal skje uten ugrunnet opphold. d. Redundans i anlegget eller kraftsystemet. 2.1.2 Tiltakene skal komplettere hverandre og gi en balansert helhet. 2.1.3 Anlegget skal fungere uavhengig av de strømutfall som kan forekomme i ordinær strømforsyning og påregnelige feil i eget strømforsyningssystem. 2.1.4 Anlegget skal kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriften, jf. § 4-2.	3.1 For transformatorstasjoner, koblingsanlegg/-stasjoner, kraftstasjoner og driftskontrollsystemer gjelder følgende krav: 3.1.1 Anleggets sikringsnivå skal ivaretas gjennom en kombinasjon av blant annet følgende tiltak: a. Alle uønskede hendelser og handlinger skal oppdages straks, kunne verifiseres og håndteres av et effektivt reaksjonsmønster. b. Fysisk og elektrisk utførelse og beskyttelse skal være på et nivå som forebygger eller forhindrer tap av funksjon og ødeleggelse. c. Gjenoppretting av eventuelle funksjonstap skal skje så raskt som fysisk mulig. d. Redundans i anlegget eller kraftsystemet. 3.1.2 Tiltakene skal komplettere hverandre og gi en balansert helhet. 3.1.3 Anlegget skal fungere uavhengig av ordinær strømforsyning og feil i anleggets eget strømforsyningssystem. Funksjon skal opprettholdes også ved upåregnelige og langvarige strømutfall. 3.1.4 Alle anlegg skal samtidig og så raskt som mulig kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriften, jf. § 4-2.

De funksjonsbaserte krav til sikringstiltak innen (a) overvåkning og effektivt reaksjonsmønster, (b), fysisk og elektrisk beskyttelse, (c) opprettholdelse og gjenoppretting av funksjon og (d) redundans i anlegg eller system skal utgjøre en balansert helhet som skissert i Figur 2.

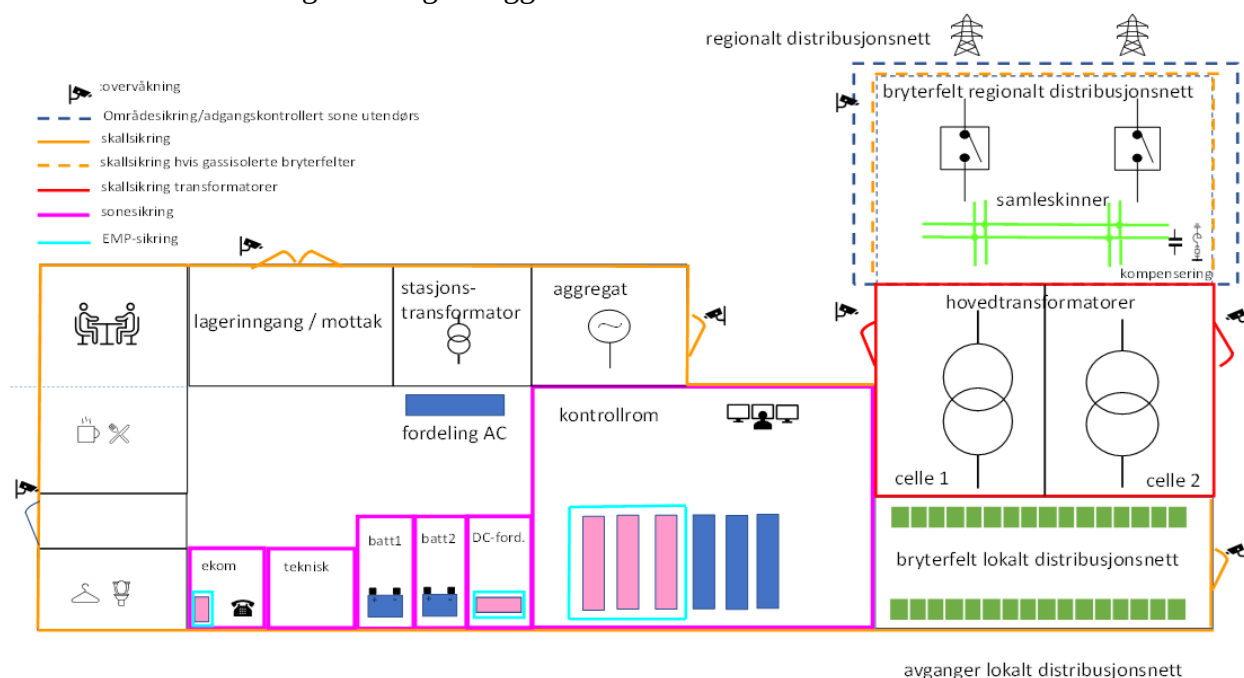


Figur 2: Funksjonsbaserte krav til overvåkning, beskyttelse, gjenoppretting og redundans for anlegg i klasse 2 og 3.

3 VEDLEGG 2 OG 3: SPESIFIKKE KRAV FOR STASJONER KL.2 OG 3:

<i>klasse 2</i>	<i>klasse 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
2.2 For transformatorstasjoner, koblingsanlegg/stasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:	3.2 For transformatorstasjoner, koblingsanlegg/stasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1
Se funksjonsbaserte krav i avsnitt 0 foran. Se veiledning til kravene 2.2.1 til 2.2.8	Se funksjonsbaserte krav i avsnitt 0 foran. Se veiledning til kravene 3.2.1 til 3.2.11

Figur 3 viser prinsippskisse for klasse 2 stasjonsanlegg. Den kan også brukes for å planlegge prinsipper for klasse 3 stasjonsanlegg, da kommer områdesikring rundt hele stasjonen i tillegg, ikke bare rundt utvendige koblingsanlegg.



Figur 3: Prinsippskisse for klasse 2 stasjonsanlegg

3.1 Oppdagelse av uønskede hendelser og handlinger

Figur 3 med prinsippskisse for klasse 2 stasjonsanlegg viser bl.a. hvilke steder i det utvendige anlegget som må overvåkes for å kunne oppdage uønskede hendelser og handlinger. Det gjelder alle steder der det er mulig å passere en område- og skall-grense, samt alle utvendige vitale anleggsdeler. I tillegg kommer systemer og prosedyrer for overvåking, alarmering av og reaksjoner på brann, røykutvikling, gasslekkasjer, oversvømmelse, osv. iht. kravene etter klasse gitt nedenfor.

klasse 2	klasse 3
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Stasjonsovervåking	
2.2.1 Anlegget skal være utstyrt med effektive og pålitelige alarmer for brann, innbrudd, elektriske feil og feil i styresystemer, samt ha etablert tiltak for effektiv reaksjon.	3.2.1 Anlegget skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmering, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger.
Det skal til enhver tid holdes kontroll på hvem som har rettmessig adgang til anlegget, i henhold til § 5-1. <i>Effektiv og pålitelig deteksjon:</i> Anlegget må, via driftskontrollsystem eller på annen måte ha systemer som løpende overvåker anleggets	<i>Effektiv og pålitelig deteksjon:</i> Alle anlegg skal ha overvåking (elektronisk, optisk eller mekanisk, alternativt vakthold) for straks å oppdage og reagere på uønskede hendelser og handlinger, og på den måten bidra til å forebygge og hindre dem. Skulle det likevel inntreffe uønskede hendelser

<i>klasse 2</i>	<i>klasse 3</i>
tekniske tilstand og drift, alarmerer om feiltilstander, og virksomheten må ha prosedyrer for nødvendig inngripen og feilretting. I tillegg til regelmessig tilsyn og gode rutiner, skal det som et minimum være installert innbrudds- og brannalarm (oppdagelse og varsling) i alle viktige deler av anlegget. <i>Verifikasjon og reaksjon:</i> Alarmene skal raskt og effektivt varsle videre til vaktentral, driftssentral eller annen vaktordning med personell som er kompetent til å følge opp den uønskede situasjonen. Virksomheten skal ha beredskap for å kunne sende ut personell raskt for stedlig verifikasjon av hendelsen og for å gjennomføre de tiltakene som situasjonen krever. Virksomheten må i tillegg ha gjennomførbare planer for skjerpet tilsyn og kontroll med anlegg i ekstraordinære situasjoner. <i>Varsling til nødetater, politi, forsvar:</i> Det skal legges til rette for varsling til og samarbeid med forsvaret, politi og andre nødetater.	eller handlinger, skal det være mulig å verifisere og dokumentere dem i ettertid. <i>Uønskede handlinger:</i> Det skal ikke være mulig å trenge seg inn i et anleggs definerte skallsikring og sikkerhetssoner uten at dette oppdages og varsles. <i>Uønskede hendelser:</i> Brann, branntilløp, røykutvikling og liknende skal oppdages og alarmeres. Øvrig system for oppdagelse og varsling av andre typer uønskede hendelser (for eksempel gasslekkasjer, oversvømmelse, varmgang, elektriske eller mekaniske feil) skal vurderes for de enkelte anlegg. <i>Verifikasjon og dokumentasjon:</i> Overvåkingen (styrbare eller faste kameraer, TV skjermer, PC eller liknede) må dekke alle vesentlige deler av anlegget, også eventuelle adkomster til fjellanlegg. Ved utløst alarm må det være opptaks og lagrunsmuligheter av data og video slik at KBO-enheten kan sikre bevis. Det må være et opptaks- og lagringssystem med så god kvalitet at nødvendige detaljer blir tydelig nok for verifikasjon <i>Rask reaksjon:</i> Systemet skal umiddelbart varsle døgnbetjent vaktentral, driftssentral, eller liknende vaktordninger som sikrer at kompetent personell kan følge opp den uønskede situasjonen umiddelbart. <i>Varsling til nødetater, politi, forsvar:</i> Det skal legges til rette for varsling til og samarbeid med politi, andre nødetater og forsvar, og at disse kan bruke overvåkningssystemet i forbindelse med utrykning, vakthold, etterforskning eller andre innsatser. <i>Tilgjengelighet under ekstraordinære situasjoner:</i> Overvåkningssystemet må ikke enkelt kunne omgås, narres eller settes ut av spill (sabotasje) uten at dette blir oppdaget. Systemene må så langt mulig også fungere i mørke og dårlig vær (vind, snø mv.).

<i>klasse 2</i>	<i>klasse 3</i>
	<i>Personvern hensyn:</i> Ved valg av system for kameraovervåkning eller liknende er det viktig å ta personvern hensyn og overholde personopplysningsloven.



Eksempel: Stasjonsovervåkning

I en transformatorstasjon i klasse 2 i tettbygd strøk var det satt opp kameraer utendørs ved alle innganger til stasjonen. Ved nærmere ettersyn viste det seg at kameraene ikke var tilkoblet med ledninger til overvåkningssystemet. For en som vil bryte seg inn, er dette lett å se. Kameraene kunne derfor ikke godtas som stasjonsovervåkning.

3.2 Fysisk beskyttelse av anlegg

Figur 3 med prinsippskisse for stasjonsanlegg viser inntegnede grenser for område-, skall-, sone- og EMP-sikring. Virksomheten bør kunne presentere en tegning der disse grensene er tegnet inn, for å tydeliggjøre hvilke barrierer, dører, porter, luker, osv. som er sikret etter hvilke krav. Det må være enkelt å redegjøre for hvilke sikringstiltak som er brukt.

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Områdesikring	
<i>(Ikke krav til områdesikring for klasse 2-anlegg, men bygges hvis det er vurdert nødvendig).</i>	3.2.2 <i>Anlegget skal ha en fysisk områdesikring som effektivt hindrer inntrengning.</i>
Områdesikring for klasse 2-anlegg, som gjerder, porter, bommer og liknende vurderes i hvert enkelt tilfelle. Det det er for eksempel nødvendig dersom skallsikringen har mangler. Se også krav om minst mulig risiko i § 5-3 og kravene under vedlegg 2.1. For anlegg i tettbebygde strøk med begrenset tilgang på areal, må eventuelle ekstra tiltak til skallsikringen vurderes, for eksempel byggkonstruksjon, arealdisposisjon og andre tiltak, f.eks. parkeringsforbud inntil skallsikringen.	Klasse 3-anlegg skal alltid ha områdesikring som den ytterste barrieren som markerer anleggsgrensen for uvedkommende, og som fysisk skal hindre eller begrense adkomsten til frittstående elementer i anlegget. <i>Utførelse:</i> Områdesikringen kan bygges med bommer, gjerder, porter, betong-/ stein-skiller, mv. For anlegg i fjell er det selve fjellet og adkomstene inn som utgjør områdesikringen. Låser, beslag, bolter og skruer skal være sikret mot enkel demontering.. <i>Bommer:</i> Der forholdene tilsier det skal kjøreadkomster være sikret med solid veibom i passe avstand fra kjøreport. Den skal bygges slik

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Bommer/ gjerder:</i> Ved kraftstasjoner vil det være naturlig å sette opp veibom eller liknende. <i>Låser:</i> Låser med tilhørende beslag og innfesting må minst tilsvare FG klasse 2 med tilsvarende soliditet i port, bom og liknende i en balansert helhet, uten glipper og svake punkter.	at det er vanskelig å kjøre rundt bommen. Bommen bør kunne stenges med lås og beslag i sikringsklasse 3 eller 4, se vedlegg 4. <i>Gjerder:</i> Høyden på gjerdet bør være på minst 2,7 meter, eller høyere hvis nødvendig pga. snømengde, terreng, el.lign. I tillegg skal det alltid vurderes ytterligere forebyggende tiltak på toppen av gjerdet, som for eksempel piggråd. Gjerdestolpene må være solid fundamentert, støpt i løs grunn, nedboret i fjell eller liknende. De må ha stram topp og bunntråd, eventuelt vinkeljern eller liknende, stramt festet i stolpene. Gjerdeduken (flettverksduk) må maksimalt ha 50 millimeter maskevidde og trådykkelse minimum 2,8 millimeter. Gjerdeduken må være godt festet i både topp-/ bunntråd og i gjerdestolpene, både med tilstrekkelig antall og solide festetråder. Alle skjøter i gjerdetråd og duk må være godt sammenføyd. Glipper i/under gjerdet må ikke forekomme. Gjerdet utføres ev. som stålstendere eller strekkmetall. <i>Gjerde- og kjøreporter:</i> Skal være like høye, solide og med like god utførelse som gjerdet. Stolper må støpes i løs grunn, bores ned eller boltes i fjell. Styringen (manuell og/eller automatisk) av portene må ikke kunne bli manipulert av uvedkommende. Tofløyede porter må ha låsbar midtsikring mot bakke. <i>Låser:</i> Portene må være utstyrt med låser og beslag i sikringsklasse 3 eller 4, og bakkantbeslag eller hengsler sikret mot avløfting. I tillegg til de ovennevnte punktene må virksomheten gjennomføre ytterligere tiltak ut fra stedlige forhold og risiko.
Avstand fra gjerdet til koblingsanlegget	
<i>(Ikke krav til områdesikring for klasse 2-anlegg, men bygges hvis det er vurdert nødvendig).</i>	3.2.3 Anlegget skal ha god avstand til ikke-avsperrede områder.
Dersom det blir bygget områdesikring for klasse 2-stasjon, bør det utføres en risikovurdering av avstand til utsatte komponenter. Kan vurdere å ha større avstand enn minstekravet i fef for å ta	Der forholdene tillater dette, bør områdesikring settes opp i en avstand på minst 30 meter («kasteavstand» for gjenstand med vekt 100 g) fra vitale komponenter. Alle elementer i områdesikringen bør holdes fri for vegetasjon, bygningselementer og andre gjenstander i en sone

<i>klasse. 2</i>	<i>klasse. 3</i>
hensyn til «kasteavstand», se nærmere i veiledningen til 3.2.3	på 3 meter til alle kanter. Alle løse gjenstander (for eksempel stiger, søppeldunker, kabeltromler, tilhengere) som kan medvirke til enkel forsering av områdesikringen må være plassert på innsiden, helst ute av syne, innelåst eller fastlåst. Om vinteren må ikke snø bli liggende inntil gjerdet. Det er viktig beholde fri gjerdehøyde.
Skallsikring Prinsipp for skallsikring er skissert i Figur 3. Skall omfatter bygningskropp, celler med stengsler, ståldører, rister, stålporter, etc. Skallet må bygges og sikres etter middels gode (kl 2) eller høye (kl 3) krav til standard/norm og etter lokal risikovurdering. Det er spesielt viktig å vurdere svake punkter som dører, vinduer, kabelføringer, luker og alle andre mulige adkomster.	
<i>2.2.2 Viktige anleggsdeler som driftsbygg, innendørs apparatanlegg, muffeanlegg og anlegg for stasjonsstrøm og styring skal ha god skallsikring etter fastsatte normer.</i>	<i>3.2.4 Viktige anleggsdeler som driftsbygg, innendørs apparatanlegg, muffeanlegg og anlegg for stasjonsstrøm og styring, samt store og viktige komponenter med lang leveringstid, skal ha god skallsikring etter fastsatte normer for sikringsnivå.</i>
Vegger og dører: Yttervegger og seksjonerende vegger skal sikres iht. brannklasse REI 60 M, dører med videre i EI 60 eller bedre. Dører som har utvendige hengsler, skal ha bakkantbeslag. Gulv, tak, mv. må sikres tilsvarende. Låser: Alle utvendige dører/porter/adkomster sikres mot avløfting og med gode låseanordninger, som et minimum sikkerhetsklasse 4 etter EN, og låser i FG klasse 3 eller bedre. Vinduer: Vinduer i skallsikringen bør unngås. Eventuelle vinduer i skallsikringen mot kontrollrom og andre rom som gir videre adgang til viktige deler av anlegget skal ha hærverkshemmende, klasse P5A, eller fortrinnsvis innbruddshemmende (klasse P6B) eller bedre, etter EN 356. Andre adkomster: Alle føringer for kabler, rør, kanaler, kulverter og andre mulige adkomster må ha skallsikring tilsvarende som nevnt ovenfor. Tilleggssikring: Virksomheten kan vurdere behov for tilleggssikring og utføre det i henhold til egne akseptkriterier og analyser av anleggets betydning	Vegger og dører: Yttervegger og seksjonerende vegger skal sikres iht. brannklasse REI 60 M, dører med videre i EI 60 eller bedre. Gulv, tak, mv. må sikres tilsvarende. Låser: Alle utvendige dører/porter/adkomster sikres mot avløfting og med gode låseanordninger av høy kvalitet som bør oppfylle sikkerhetsklasse 5 etter EN og låser med mer i FG klasse 4 eller bedre. Vinduer: Vinduer i skallsikringen bør unngås og rom for kontrollutrustning kan ikke ha vinduer. Eventuelle vinduer i andre rom som gir videre adgang til viktige deler av anlegget, skal ha innbruddshemmende glass i klasse P7B eller bedre, etter EN 356. Andre adkomster: Alle føringer for kabler, rør, kanaler, kulverter og andre mulige adkomster må ha skallsikring tilsvarende som nevnt ovenfor. Tilleggssikring: Virksomheten må vurdere behov for tilleggssikring og utføre det i henhold til egne akseptkriterier og analyser av anleggets betydning og lokal risiko. For eksempel kan virksomheten bygge sterkere konstruksjoner ved å øke betong-

<i>klasse. 2</i>	<i>klasse. 3</i>
og lokal risiko. For eksempel kan virksomheten bruke tiltak som gjelder for sikring av anlegg i klasse 3.	tykkelse og -kvalitet, styrke armeringen, øke belastningsevne, forsterke gitter, øke kvaliteten på låser, osv.
Skallsikring av gassisolert koblingsanlegg (GIS) (gjelder for både klasse 2 og 3) GIS-anlegg må ha skallsikring på nivå tilsvarende krav 2.2.2 / 3.2.4. Det er viktig med bedre skallsikring av GIS-anlegg enn av tradisjonelt luftisolert anlegg (AIS). Det skyldes lengre reparasjonstider og avhengighet av utenlandsk kompetanse og spesialdeler. Videre er det for GIS-anlegg mindre muligheter for improvisasjoner med om-/forbi-koblinger og ombytte/rokking av ødelagte/skadede enkeltstående komponenter. Selv om viktige GIS-anlegg bygges redundante og dels er seksjonerte, vil særlig bevisst skadeverk, men også brann og andre større hendelse, lett kunne sette hele anlegget ut av spill. Virksomheten må også ta hensyn til mulig følgeskader som ukontrollert lekkasje av SF6-gass. I en vurdering av sikringstiltak med ulike barrierer, kan til en viss grad det ene tiltaket kompensere for svakheter i det andre. Risikomessig gunstig beliggenhet i omgivelser, plassering i terrenget, god områdesikring, overvåkningssystem mv kan i noen grad veie opp for en svakere skallsikring. Likevel må det være en viss balanse mellom de ulike komponentene i sikringssystemet. Kravet til et solid brannfast/-sikkert bygg med god innbruddsikring etter klasse må likevel være oppfylt. Som for transformatorceller, se krav 2.2.4 / 3.2.6, kan NVE for GIS-anlegg akseptere at det benyttes ekvivalenter til 20 cm dobbelarmert betong i form av et bygg oppført av elementer, gitt at disse gis solid sammenføyning, og ellers oppfyller sin funksjonsbaserte hensikt som skallsikring etter klasse iht. forskriften.	
Sonesikring En sone er et avgrenset rom/område, f.eks. kontrollrom, data/sambandsrom, rom for nødstrøm, beredskapsrom og lignende. Sonen sikres etter anleggets klasse, viktigheten av utstyret i sonen og nivået på ytre skallsikring. Hovedhensikten med slik sonesikring, er et ekstra lag med fysisk sikring mot uvedkommende rundt særlig viktige eller sårbare anleggsdeler.	
2.2.3 Driftskontrollrom og andre rom for styring og samband skal være egne adgangskontrollerte soner med middels sikringsnivå og brannmotstand etter fastsatte normer.	3.2.5 Driftskontrollrom, datarom og andre rom for styring og samband skal være egne adgangskontrollerte soner, godt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand
Sonesikring omfatter særlige viktige områder/rom for lokalkontroll, samband, nødstrøm og liknende. Sikringsnivået skal tilpasses viktigheten av utstyret i sonen og nivået på den ytre skallsikringen, normalt minst FG-klasse 3 eller sikringsklasse 3 eller 4 etter EN 1627. Se også veiledning om adgangskontroll for uvedkommende til § 5-1 om sikringsplikt.	Sonesikring omfatter særlige viktige områder/rom for lokalkontroll, samband, nødstrøm og liknende. Sikringsnivå tilpasses viktigheten av utstyret i sonen og nivået på den ytre skallsikringen, normalt minst FG-klasse 3 eller 4 og sikringsklasse 4 etter EN 1627. Se også veiledning om adgangskontroll for uvedkommende til § 5-1 om sikringsplikt.

<i>klasse. 2</i>	<i>klasse. 3</i>
Sikring av hovedtransformatorer De største hovedtransformatorene er særlig viktige og tunge komponenter med svært lange reparasjons- og erstatningstider, så er det spesielt strenge krav til sikring av disse.	
<i>2.2.4 Alle hovedtransformatorer med tilhørende adkomster skal sikres fra alle kanter med bygg eller lignende, med god beskyttelse etter fastsatte normer for sikring og brannmotstand.</i>	<i>3.2.6 Alle hovedtransformatorer skal skallsikres fra alle kanter til over topp endemuffer ved hjelp av fjell eller transformatorceller av solid dobbeltarmert betong eller tilsvarende, og være konstruert og oppført etter anerkjente byggenormer. De skal herunder beskyttes og seksjonerer med høy brannmotstand etter fastsatt norm. De skal ha låsbare dører/porter eller fast montert gitter med høyt sikringsnivå etter fastsatt norm i alle mulige adkomster og lufteåpninger opptil minimum tre meter fra bakkeplan eller liknende.</i>
Transformatorene skal ha sideveis beskyttelse fra alle kanter, i form av fast terreng eller konstruksjon. Konstruksjon i betong skal være minimum 160 mm armert plaststøpt eller prefabrikkerte armerte elementer montert i konstruksjon med solide avstivninger, sammenføyninger, mm. Alternativ til betong er stål (dekningstykkelse minimum 10 millimeter. Stålkvalitet bør oppfylle HB 200 eller ekvivalenter i aluminium. Sidebeskyttelsen skal skjule transformatorene opp til topp endemuffer. Konstruksjonen bør som et minimum tåle en belastning på 2 kN/m² eller mer fra alle kanter. Det skal være seksjonering mellom hver enkelt transformator. Vegger i konstruksjon, inkludert skillevegger mellom transformatorer, utføres minimum i brannklasse REI 90 M (M om relevant), og seksjonerende dører med videre i brannklasse EI 90 eller bedre. Lokal betjening (brytere, tappekran for olje, mm.) må være innenfor samme sikringsnivå.	Transformator til og med topp endemuffer bør så langt mulig gis skjul og dekning i god avstand (flere hundre meter) sett fra omgivelsene. Dekning kan bestå av fast terreng eller av konstruksjon. Ved terreng må transformator i tillegg beskyttes av konstruksjon med utvendig høyde på minst tre meter over terreng. Konstruksjon i betong skal være minimum 200 mm armert plaststøpt betong eller prefabrikkerte armerte elementer montert i konstruksjon med solide avstivninger, sammenføyninger, mm. Betongfasthet B30 eller bedre og armering tilsvarende sveiset nett K357 eller bedre. Alternativ til betong er stål (dekningstykkelse minimum 20 millimeter, stålkvalitet bør oppfylle HB 200 eller ekvivalenter i aluminium. Konstruksjonen bør tåle en belastning på 4 kN/m² eller mer fra alle kanter Hver transformator seksjonerer i egen konstruksjon beskyttet på alle kanter. Vegger i konstruksjon, inkludert seksjonerende vegger mellom flere transformatorer, utføres minimum i brannklasse REI 120 M (M – om relevant), og seksjonerende dører med videre i brannklasse EI 120 eller bedre.

<i>klasse. 2</i>	<i>klasse. 3</i>
Dører, låser, gitter, kabelføringer, osv skal være sikret på samme nivå som ovennevnte skallsikring for klasse 2. Se også forskrift om elektriske forsyningsanlegg (fef) § 4-9 om sikkerhetstiltak og sikkerhetsutstyr.	Konstruksjon kun basert på murverk, hul- eller lettbetongblokker oppfyller ikke forskriftens krav. Alle monterte elementer monteres med bolter, mv. slik at de ikke kan fjernes fra utsiden. Se også forskrift om elektriske forsyningsanlegg (fef) § 4-9 om sikkerhetstiltak og sikkerhetsutstyr.

3.3 Redundans

Redundans innebærer at det skal finnes annen komponent eller system som automatisk eller ved rask manuell omkobling kan overta funksjonen til den anleggsdelen som har feil eller er ødelagt.

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Redundans i høyspenningsanlegg Viktige kraftforsyningsanlegg må være dimensjonert slik at én enkelt feil eller hendelse ikke skader eller hindrer anleggets vitale funksjoner i det kraftsystemet det er en del av. <i>Redundans i anlegg:</i> En metode er å ha dobbelt sett av viktige komponenter (for eksempel hovedtransformatorer, samleskinner og brytere) – gjerne i kombinasjon med fysisk og elektrisk atskillelse enten ved avstand eller fysisk beskyttelse. Eksempelvis kan man plassere (minst) to hovedtransformatorer (for et gitt spenningsnivå) i hver sin transformatorcelle, som hver for seg kan ta den normallasten anlegget er dimensjonert for. Sannsynligheten for at begge havarerer samtidig er liten. <i>Redundans i system:</i> Alternativt kan redundans ordnes ved at et annet anlegg kan overta det vesentlige av funksjonen til et havarert anlegg – for eksempel at det finnes to alternative transformatorstasjoner i et forsyningsområde. Manglende redundans kan i noen grad kompenseres ved å øke evnen til rask gjenoppretting ved for eksempel en planlagt og fysisk forberedt forbi-/omkobling. <i>Redundans i anlegg bygd før 1.1.2013:</i> Der det fysisk er svært krevende eller blir uforholdsmessig kostbart krever NVE ikke ombygging eller anskaffelse av tyngre komponenter for å oppnå redundans i høyspenningsanlegg. Dette er ofte forholdet ved eldre transformatorstasjoner i tett bebyggelse. Manglende redundans må i så fall kompenseres ved blant annet beredskapsplaner iht. til § 2-4 og reparasjonsberedskap iht. § 4-1. For eksempel skal det foreligge en konkret plan for hvordan hovedtransformatoren kan erstattes av en annen. Ved manglende redundans i koblingsanlegget (brytere, samleskinne og liknende) må det foreligge planer, utstyr, reservedeler og kompetanse for rask forbikobling til ordinær gjenoppretting har funnet sted.	
2.2.6 Skal som hovedregel ha dublering av de viktigste komponenter for anleggets primære funksjoner. Dette gjelder bl.a. samleskinner, skillebrytere, samt annen nødvendig utrustning.	3.2.8 Anlegget skal som hovedregel ha dublering av de viktigste komponenter for anleggets primære funksjoner. Dette gjelder bl.a. samleskinner, effekt- og skillebrytere, samt annen

<i>klasse. 2</i>	<i>klasse. 3</i>
	<i>nødvendig utrustning. Hovedtransformatorers funksjon skal ha redundans i anlegg eller system.</i>
Det kreves ikke dublering av hovedtransformatorer, men anlegget skal tåle utfall av den største transformatoren uten at det går ut over strømforsyningen. Det kan være hensiktsmessig å bruke tre transformatorer, hver på 20 MVA i stedet for to på 30 MVA hvis største last ikke overskrider 40 MVA. Dette er allikevel ikke nødvendig hvis all last kan dekkes med redundans i systemet.	Det kreves ikke dublering av hovedtransformatorer, men anlegget skal tåle utfall av den største transformatoren uten at det går ut over strømforsyningen. Det kan være hensiktsmessig å bruke fire transformatorer, hver på 150 MVA i stedet for tre på 200 MVA hvis største last ikke overskrider 450 MVA. Dette er allikevel ikke nødvendig hvis all last kan dekkes med redundans i systemet.
<i>Redundans, stasjonsstrøm og styresignaler</i>	
<i>2.2.5 Anlegget skal ha dublerte føringer for stasjonsstrøm og styresignaler.</i>	<i>3.2.7 Anlegget skal ha dublerte og fysiske uavhengige kabelføringer for hhv. styring og samband, nød- og stasjonsstrøm og høyspent, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.</i>
Kravet er en ytterligere konkretisering for klasse 2, se også veiledningen ovenfor, som gjelder både klasse 2 og 3.	Kravet er en ytterligere konkretisering for klasse 3, se også veiledningen ovenfor, som gjelder både klasse 2 og 3.
<i>Dublering, separering og seksjonering av viktige kabler</i>	
<i>2.2.8 Viktige kabler for driftskontroll og styre- og nødstrøm skal så langt som mulig, fysisk separeres fra høyspentkabler.</i>	<i>3.2.10 Dublering etter punkt 3.2.7 til 3.2.9 skal så langt som mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.</i>
Kravet er en ytterligere konkretisering for klasse 2, i tillegg til veiledningen ovenfor, som gjelder både klasse 2 og 3.	Kravet er en ytterligere konkretisering for klasse 3, i tillegg til veiledningen ovenfor, som gjelder både klasse 2 og 3.

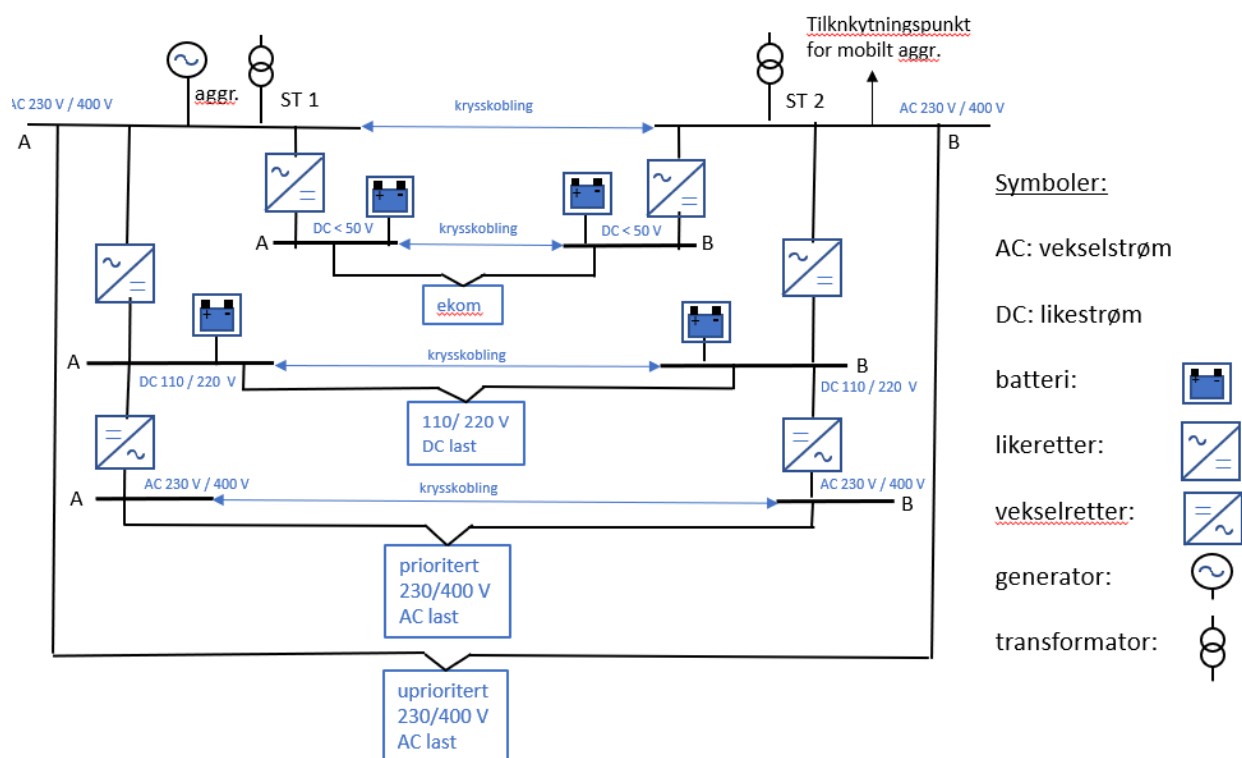
3.4 Stasjonsstrøm og nødstrømsanlegg

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Strømforsyning til selve stasjonen og til alle hjelpefunksjoner er normalt forsynt fra nettet via stasjonens krafttransformatorer (tertiærvikling) levert til stasjonstransformator eller fra nettstasjon tilknyttet lokalt distribusjonsnett. Stasjonsstrøm omfatter stasjons-/nettransformatorene, AC lavspent hovedfordeling, underfordelinger og strømkabler, like/vekselrettere med DC lavspent underfordeling og kabling, svakstrøm (< 50V) med transformering, fordeling og kabling. Nødstrøm med batteribanker	

<i>klasse. 2</i>	<i>klasse. 3</i>
(220 /110 V, eventuelt også 48 /24 V), og nødstrømsaggregat, samt opplegg for tilkobling av mobilt aggregat. Det skal være tilgang på strøm for å betjene viktige driftsfunksjoner og viktige HMS-funksjoner både ved ordinær strømforsyning og ved bortfall av denne. Strømforsyningsanlegg, inkludert nødstrømsanlegg, må være konstruert og plassert slik at risikoen for skade og uhell blir minst mulig. Det må også kunne tåle de maksimale belastningene som det kan bli utsatt for. Anlegget bør ha prioriterte kurser for de viktigste funksjonene, slik som styrestrøm, kontrollrom og belysning i viktige deler av anlegget. Ved alle anlegg må det foreligge en risikovurdering av strømforsyningen til anlegget og dets kontrollfunksjoner, sambandsanlegg mv. i tråd med anleggets klasse og betydning for forsyningssikkerheten. Løsninger for nødstrøm med nødvendig dublering, avbruddsfri forsyning og total opptid må være inkludert i vurderingen. Vurdering av tilgjengelighet for adkomst, betjening, klimatiske og geografiske forhold må også være inkludert. Strømforsyningsanlegget og nødstrømsanlegget skal holdes i forsvarlig og driftssikker stand. Funksjon, kapasitet og utholdenhet må testes med jevne mellomrom. Minst en gang i året bør nødstrømsanlegget testes fullt ut med all prioritert last og ved at ordinær strømforsyning kobles fra.	
<i>Dublering og avbruddsfri strømforsyning</i>	
<i>2.2.7 Skal ha et dublert nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Om det ikke er installert et stasjonært nødstrømsaggregat, må et mobilt aggregat kunne kobles til innenfor batteritiden under maksimal belastning. Anlegget må samlet sett ha en gangtid på minst to døgn.</i>	<i>3.2.9 Anlegget skal ha et elektrisk og fysisk dublert system for egen stasjonsstrøm med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften av stasjonen forsynes fra to helt uavhengige og separerte strømkurser-/ systemer. Dette skal også omfatte et nødstrømsystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning og minimum har en samlet driftstid på minst seks timer. Det skal være installert et stasjonært nødstrømsaggregat med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrudd og minst tre døgns selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte. Nødstrømsystemet skal tåle de maksimalbelastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling av nødvendig utstyr og liknende.</i>
Kravet er en ytterligere konkretisering for klasse 2, i tillegg til fellesveiledningen gitt til både klasse 2 og 3 ovenfor.	Kravet er en ytterligere konkretisering for klasse 3, i tillegg til fellesveiledningen gitt til både klasse 2 og 3 ovenfor.

<i>klasse. 2</i>	<i>klasse. 3</i>
Dublering: Dublering for nødstrøm kan skje på flere måter. To eksempler som oppfyller kravet er: 1. To batterier i samme rom. To likerettere og to vekselrettere i et annet rom. Tilkobling av mobilt aggregat. 2. Stasjonært aggregat pluss ett batteri med like- og vekselretter. Batteri og aggregat i egne rom. Forøvrig må dublering av nødstrøm planlegges i henhold til vurdering av risikoen for å miste avbruddsfri strømforsyning. Se også REN-blad 7007 om lokal strømforsyning til transformatorstasjoner. Gangtid: Batterianleggene/ UPS skal ha en samlet driftstid på minimum 6 timer. Driftstid for batterianlegget kan reduseres til minimum 3 timer dersom det er installert et stasjonært nødstrømsaggregat. Total gangtid for nødstrømsforsyning (batteri og aggregat) skal være minst 2 døgn Nødaggregat: mobilt nødstrømsaggregat skal kunne kobles til og være tilgjengelig innenfor driftstiden for batteriet. Det må her tas hensyn til den påregnelig tid for feilretting om aggregatet ikke starter. Man skal vurdere å dublere batteri-/ UPS-systemet helt eller delvis. Dimensjonerende belastning må også vurderes.	Figur 4 viser et prinsipp som vil være dekkende for å tilfredsstille krav til stasjonsstrøm og nødstrøm for stasjoner i klasse 3. Dublering I tillegg til dublert strømforsyning omfatter kravet også dublering med uavhengige batterianlegg/UPS. De dublerte anleggene skal være både elektrisk og fysisk uavhengige. Gangtid: Batterianleggene/ UPS skal som et minimum ha en driftstid på minst 6 timer. Total gangtid for nødstrømsforsyning (batteri og aggregat) skal være minst 3 døgn Nødaggregat: Det skal være installert et stasjonært nødstrømsaggregat med automatisk oppstart ved strømbrudd. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære aggregatet skulle svikte.

Figur 4 viser en prinsippskisse for stasjonsstrøm og avbruddsfri nødstrøm. Figuren inneholder alle elementer som bør inngå i en klasse 3 stasjon: Stasjonstransformator, nødstrømsaggregat, avbruddsfri strømforsyning, ekom, likestrømslast, prioritert og uprioritert vekselstrømslast. Alternativ til å bruke vekselstrømsretter til prioritert vekselstrømslast er å ha all prioritert last som likestrømslast. Figuren viser alle elementer i dublert utførelse. A- og B-siden av samleskinnene må være fysisk adskilt. Det er også vist mulighet for krysskobling mellom A- og B-siden for alle nivåer (DC 48V, DC 110 V og AC 230, ev. 400 V). Grad av dublering for klasse 2 stasjon gjøres i henhold til risikovurdering, se også veiledningen til krav 2.2.7.



Figur 4: Prinsippskisse for dublert stasjonsstrøm og dublert avbruddsfri nødstrøm for klasse 3-stasjon

Eksempel: Opprettholde forsyningen ved hjelp av krysskobling mellom samleskinner

Det har oppstått en brann, stasjonstransformatoren ST 1 har havarert og hovedfordeling A er ute av drift. Samtidig er vekselretteren på samleskinne B utkoblet for vedlikehold. Den prioriterte vekselstrømslasten får likevel uavbrutt strømforsyning fra stasjonstransformator 2 over krysskoblingen mellom likerettersamleskinnene A og B og deretter gjennom vekselretteren.

Se Figur 5 Anleggsdeler som er ute av drift er markert med rødt. Forsyningsveien fra samleskinne B til prioritert last er markert med grønt.



<i>klasse. 2</i>	<i>klasse. 3</i>
	Denne strømmen flyter parallelt i de tre fasene og til jord gjennom nullpunktet. Dette fører til metning i kjernen, og spenningen avviker fra sinusform. Mengden med overharmoniske på høy- og lavspentsiden må analyseres, og virkningen av de overharmoniske på vern- og kontrollutrustning og på kompenseringssanlegg må vurderes. Metningen i kjernen og påvirkningen på spenningsformen fører til økt behov for reaktiv effekt. Konsekvensen av dette må vurderes og tiltak iverksettes for å unngå spenningskollaps. Det må lages en plan for hvordan varsler om solstorm kan brukes og hvilke tiltak som er relevante for beskyttelse, se krav gitt i § 5-3. SINTEF har laget en rapport om tiltak for å motvirke konsekvenser og håndtere risiko knyttet til geomagnetisk induisert strøm i kraftnettet, se NVE ekstern rapport nr. 15/2021.

4 VEDLEGG 2 OG 3: TILLEGG FOR KRAFTSTASJONER, KL. 2 OG 3

4.1 Kraftstasjoner bygget i fjell

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
<i>Kraftstasjoner bygget i fjell</i>	
2.3 For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 2.1:	3.3 For kraftstasjoner gjelder følgende krav i tillegg til kravene i punkt 3.1:
Se funksjonsbaserte krav i punkt 2.1. Se veiledning til kravene 2.3.1 til 2.3.10.	Se funksjonsbaserte krav i punkt 3.1. Se veiledning til kravene 3.3.1 til 3.3.9.
2.3.1 Kraftstasjoner i fjell skal ha en adgangskontrollert og fysisk sikret sone omfattende alle adkomster. Denne sonen skal oppfylle krav til godt sikringsnivå etter fastsatte normer for sikring. Herunder skal alle stasjoner ha minst én solid og låsbar stålport eller lignende i alle adkomster.	3.3.1 (første og annet punktum) Alle vitale komponenter skal legges i beskyttende fjellrom og det skal etableres en omsluttende adgangskontrollert og fysisk sikret sone som omfatter alle mulige adkomster med høyt sikringsnivå etter fastsatt norm. Herunder skal alle stasjoner ha minst én solid og låsbar stålport eller lignende i alle adkomster.

<i>klasse. 2</i>	<i>klasse. 3</i>
Kraftstasjon klasse 2 med vitale komponenter (se klasse 3) plasseres i beskyttende fjellrom. Dersom kraftverkstransformatorer og liknende plasseres i dagen bør disse seksjoneres og beskyttes som transformator klasse 2 med nødvendige lokale tillempninger. Forutsatt at plasseringen i fjell gir solid beskyttelse, omfatter skallsikring mulige adkomster som drifts-, transport-, og andre adkomsttunneler, kabel- og ventilasjonssjakter samt andre åpninger som blant annet tverrslag og avløpstunneler. <i>Områdesikring</i> som gjerder/porter og bommer og liknende skal vurderes i hvert enkelt tilfelle. I henhold til egne akseptkriterier og ut fra lokal analyse av anleggets betydning og risiko skal man vurdere å gjennomføre ulike permanente forsterkninger av grunnsikringen. Dette kan være elementer fra grunnsikring kraftstasjon klasse 3. For kraftstasjon i fjell skal det defineres en gjennomgående helhetlig sikringssone som omfatter alle mulige adkomster. Denne sikres med barrierer, som minimum bør oppfylle sikkerhetsklasse 4 etter EN og låser med videre etter FG klasse 3. <i>Adkomster</i> eller liknende som kan lukkes permanent (eksempelvis tverrslag), bør støpes igjen med minimum 200 millimeter plass-støpt dobbeltarmert betong eller ekvivalenter i stål eller aluminium. Konstruksjoner kun basert på murverk, hul-, lettbetongblokker eller liknende oppfyller ikke forskriftens krav. <i>Vinduer i skallsikring</i> skal minst utføres som innbruddshemmende, P6B etter EN 356 eller bedre. <i>Ytre komponenter/anleggsdeler</i> sikres som for kraftstasjon klasse 2 i dagen.	Kraftstasjon i klasse 3 skal plasseres i beskyttende fjellrom. Dette gjelder alle deler av kraftstasjonen som ivaretar vitale funksjoner fra og med tilløpstunnel, trykksjakt med ventil/lukekammer, turbin, generator - til og med henholdsvis kraftverkstransformator og avløpstunnel, samt rom for styresystemer, samband og intern strømforsyning. Der kraftstasjon helt eller delvis må plasseres i dagen, se krav til sikring for kraftstasjon i dagen. Forutsatt at plasseringen i fjell gir solid beskyttelse, omfatter skallsikring mulige adkomster som drifts-, transport-, og andre adkomsttunneler, kabel-, ventilasjonssjakter og andre åpninger, samt tverrslag og avløpstunneler. For <i>alle adkomster</i> skal det defineres en gjennomgående helhetlig sikringssone. Denne sikres med solide barrierer, som minimum bør omfatte én eller flere kombinasjoner av følgende alternativer: • Heldekkende (vegg til vegg, gulv til tak) stålgritter, for adkomster kommer i tillegg solid innfestet stålport eller ståldør. • Solid stålgritter med profil tilsvarende min. 60 x 6 millimeter med senteravstand ca. 80 millimeter + avstivninger. • Solide dører/porter med tykkelse tilsvarende 10 mm stål (KD/KP 10) eller tilsvarende. • Dører/porter skal sikres mot avløfting og med låseanordninger av høy kvalitet som bør oppfylle sikkerhetsklasse 5 etter EN og låser med videre etter FG klasse 4 eller bedre. Tofløyede porter skal sikres med midtsikring oppe og nede av tilsvarende kvalitet. • Adkomster eller liknende (eksempelvis transportganger) som bare unntaksvis skal kunne åpnes, kan alternativt sikres med heldekkende armert betongvegg med bjelkestengsel i transportåpning eller tilsvarende i stål eller aluminium. • Betongtykkelse i vegger og bjelkestengsler skal være minimum 200 millimeter. Betongkvalitet minimum B 30. Armering vegg tilsvarende sveiset nett K 189 eller bedre, ekvivalent armering for bjelkestengsel.

<i>klasse. 2</i>	<i>klasse. 3</i>
	- Adkomster eller liknende som kan lukkes permanent (for eksempel tverrslag), bør støpes igjen med minimum 200 millimeter plasstøpt dobbeltarmert betong. Betongkvalitet B 30 eller bedre. Armering tilsvarende sveiset nett K 189 eller bedre. I tverrslag må selve stengslet mot vanntrykk dimensjoneres for dette. <i>Nødløsning med stålplater dersom det ikke er mulig å bygge dobbeltarmert betong i eksisterende bygg:</i> I stedet for 200 millimeter betong kan ekvivalenter i 20 millimeter stålplater benyttes. Ekvivalenter i aluminium kan vurderes. Stål og aluminium må være av god kvalitet siden legering med videre er helt avgjørende for hardhet og strekkfasthet. Stål eller aluminiumsplater/-bjelker må festes (boltes fra innsiden eller liknende) slik at disse ikke kan fjernes eller løftes ut av feste/føringer fra utsiden. <i>Alle barrierer i skallsikring skal ikke ha vinduer og bør som et minimum tåle) belastning på 4 kN/m² eller mer fra alle kanter.</i> Konstruksjon kun basert på murverk, hul- eller lettbetongblokker eller liknende oppfyller ikke forskriftens krav. For alle adkomster beregnet for hyppig/daglig, bruk bør det i tillegg til ovennevnte være en ytre sikring/barriere i form av låsbare rulleporter eller gangdører i sikkerhetsklasse 2 eller 3 etter EN, samt eventuelt ytre luker, rister med videre av tilsvarende kvalitet. Slike ytre innganger skal sikres med tilfredsstillende låseanordninger, sikkerhetsklasse 3 etter EN og låser med videre etter FG klasse 2 eller bedre. Finnes ikke slik ytre sikring, bør sikkerhetsklassen (EN/FG) heves i skallsikringens adkomster. Andre komponenter skal sikres som følger: - Vitale utendørs komponenter som inntaksluker, andre tappeanordninger, tverrslag og vannvei og avløp for kraftstasjonens drift og sikkerhet sikres med betonghus, gitter, ståldører og låser etter krav som for tilsvarende barrierer i skallsikring.

<i>klasse. 2</i>	<i>klasse. 3</i>
	• Kraftverkstransformatorer, fortrinnsvis én per generator, plasseres innvendig i fjellhall adskilt fra generator-/turbinhall og øvrig adkomst. De skal seksjoneres fra hverandre og øvrig stasjon med vegger/bjelkestengsler og dører som minimum bør ha brannklasse REI 120 (M – hvor dette relevant). Se også krav til brannsikkerhet. • Rom for kontroll, styring, samband, nødstrøm og likende skal sikres med vegger og låsbare dører som minimum bør ha brannklasse REI 60 (M) og EI 60. Se også krav til brannsikkerhet. <i>Tilleggssikring</i> Ut fra lokal analyse av anleggets betydning og risiko vurderes og iverksettes ulike permanente forsterkninger av grunnsikringen. Særlig for steder som ikke kan overvåkes eller for særlig eksponerte anlegg eller komponenter, er dette relevant. Dette kan være ulike kombinasjoner av for eksempel: • Dører/ porter/ gitter og andre stengsler forsterkes eller dubleres og sikres med låseanordninger av høyere kvalitet/ sikkerhetsklasse. • Øvrige konstruksjonsdelers evne til å tåle ulike belastninger og inntrengingsforsøk styrkes. <i>Sonesikring</i> omfatter særlig viktige områder/ rom for lokalkontroll, samband, nødstrøm og liknende. Sikringsnivået skal tilpasses viktigheten av utstyret i sonen og nivået på den ytre skallsikringen, normalt minst FG-klasse 3 eller 4 og sikringsklasse 4 etter EN 1627.

4.2 Kraftstasjoner bygget i dagen

klasse. 2	klasse. 3
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Kraftstasjoner i dagen	
2.3.2 Kraftstasjoner i dagen skal ha god fysisk sikring med minimum et solid bygg med dører/porter, vinduer og øvrige adkomster etter fastsatte normer for sikringsnivå.	3.3.1 (tredje punktum) Vitale komponenter som må legges i dagen, sikres som for transformatorstasjon, koblingsanlegg, mv. i klasse 3.
Kraftstasjoner i dagen med alle ytre komponenter/innganger av betydning for drift og sikkerhet, skal sikres med solide bygg og beskyttende konstruksjoner. Mulige adkomster sikres med luker, rister eller liknende som minst oppfyller sikkerhetsklasse 3 etter EN. Tilsvarende sikres bruksinnganger med dører, porter og liknende som minst oppfyller sikkerhetsklasse 3 etter EN og utstyres med låser etter FG klasse 2 eller bedre. Vinduer skal være hærverkshemmende (P5A) eller fortrinnsvis innbruddshemmende, (P6B) etter EN 356. Sonesikring omfatter særlige viktige områder/rom for lokalkontroll, samband, nødstrøm og lignende. Sikringsnivå tilpasses viktigheten av utstyret i sonen og nivået på ytre skallsikring, normalt minst FG-klasse 3, eller sikringsklasse 3 eller 4 etter EN 1627.	Det skal ikke være noen klasse 3 kraftstasjoner som er bygget i dagen. For vitale komponenter som må legges i dagen, se veiledning til kravene 3.2.1 til 3.2.11
Vitale komponenter plassert utendørs	
2.3.3 For kraftstasjoner i fjell og i dagen skal vitale komponenter som må plasseres utendørs, sikres etter samme krav som for transformatorstasjon, koblingsanlegg mv. i klasse 2.	3.3.1 (tredje punktum) Vitale komponenter som må legges i dagen, sikres som for transformatorstasjon, koblingsanlegg mv. i klasse 3.
Vitale komponenter utendørs for kraftstasjoner klasse 2 skal ha fysisk beskyttelse tilsvarende som for stasjonsanlegg klasse 2, se veiledning til krav 2.2	Vitale komponenter utendørs for kraftstasjoner klasse 3 skal ha fysisk beskyttelse tilsvarende som for stasjonsanlegg klasse 3, se veiledning til krav 3.2

4.3 Overvåkning, brannsikring og sonesikring i kraftstasjon

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Overvåkning av kraftstasjon	
<i>2.3.4 Anleggets adkomster og vitale områder skal være utstyrt med effektive og pålitelige alarmer for brann, innbrudd, elektriske feil, og feil i styresystemer, samt ha etablert effektiv reaksjon for slike uønskede hendelser og handlinger.</i>	<i>3.3.3 Skal ha utstyr og prosedyrer for effektiv deteksjon, alarmer, verifikasjon og reaksjon mht. uønskede hendelser og handlinger. Som et minimum skal dette omfatte adkomster og stasjonens vitale områder.</i>
Kraftstasjoner klasse 2 skal ha overvåkning tilsvarende som for stasjonsovervåkning for klasse 2 stasjoner, se veiledning krav 2.2.1.	Kraftstasjoner klasse 3 skal ha overvåkning tilsvarende som for stasjonsovervåkning for klasse 3 stasjoner, se veiledning til krav 3.2.1.
Brannsikring av kraftstasjon	
<i>2.3.5 Anlegget skal brannsikres og seksjoneres på hensiktsmessig måte med god brannmotstand etter fastsatt norm.</i>	<i>3.3.2 Anlegget skal seksjoneres på en hensiktsmessig måte med brannsikring som gir høy brannmotstand etter fastsatte normer og relevante forskrifter.</i>
Kraftstasjoner klasse 2 skal ha brannsikring og seksjonering i brannceller tilsvarende klasse 2 stasjoner, se veiledning til krav 2.2.4	Kraftstasjoner klasse 3 skal ha brannsikring og seksjonering i brannceller tilsvarende som for stasjonsovervåkning for klasse 3 stasjoner, se veiledning til krav 3.2.6.
Sonesikring i kraftstasjon	
<i>2.3.6 Driftskontrollrom, rom for styring og samband og lignende skal være egne og godt beskyttede adgangskontrollerte soner etter fastsatte normer for sikring og brannmotstand.</i>	<i>3.3.4 Driftskontrollrom, rom for styring og samband og lignende skal være egne adgangskontrollerte godt beskyttede soner etter fastsatte normer for hhv. fysisk sikring og brannmotstand.</i>
Kraftstasjoner klasse 2 skal ha sonesikring tilsvarende som for stasjonsovervåkning for klasse 2 stasjoner, se veiledning til krav 2.2.5	Kraftstasjoner klasse 3 skal ha sonesikring tilsvarende som for stasjonsovervåkning for klasse 3 stasjoner, se veiledning til krav 3.2.5
Tiltak mot geomagnetisk induuerte strømmer	
	Se veiledning til krav 3.2.11

4.4 Redundans, stasjonsstrøm og nødstrøm i kraftstasjon

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Redundans i kraftstasjon	
2.3.7 Anlegget skal som hovedregel ha dublering av de viktigste komponenter og annen nødvendig kontrollutrustning, samt ha dublerede føringer for stasjonsstrøm og styresignaler. Det kreves ikke redundans for anleggets hovedkomponenter, som turbin, generator mv.	3.3.5 Anlegget skal ha dublerede og fysiske uavhengige kabelføringer for hhv. styring og samband, nød- og stasjonsstrøm og høyspent, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.
Kraftstasjoner klasse 2 skal ha redundans tilsvarende som for redundans for klasse 2 stasjoner, se veiledning krav 2.2.6.	Kraftstasjoner klasse 3, unntatt hovedkomponenter som turbin, generator mv, skal ha redundans tilsvarende som for redundans for klasse 3 stasjoner, se veiledning krav 3.2.8.
Kraftstasjonens hovedkomponenter (turbin, generator, mv.)	
	3.3.8 Det kreves ikke redundans for anleggets hovedkomponenter, som turbin, generator mv.
Se krav 2.3.7 angående hovedkomponenter som turbin, generator mv.	Se krav 3.3.5 for krav til redundans for øvrige komponenter.
Stasjonsstrøm og nødstrøm i kraftstasjon	
2.3.8 Skal ha et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning. Om det ikke er installert et stasjonært nødstrømsaggregat, må et mobilt aggregat kunne kobles til innenfor batteritiden under maksimal belastning. Anlegget må samlet sett ha en gangtid på minst to døgn.	3.3.6 Skal ha et elektrisk og fysisk dublert system for egen stasjonsstrøm med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften av stasjonen, forsynes fra to uavhengige og separerte strømkurser-/systemer. Dette skal også omfatte et nødstrømssystem som er dublert med uavhengige batteribanker og avbruddsfri strømforsyning, og minimum har en samlet driftstid på minst seks timer. Stasjonen skal være utstyrt med en stasjonær selvdrevet anordning for stasjonsstrøm (nødstrømsaggregat, hjelpegenerator eller lignende) med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strømbrytning og minst tre døgns selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom den stasjonære anordning skulle svikte. Nødstrømssystemet skal tåle de maksimalbelastninger det kan bli utsatt for,

klasse. 2	klasse. 3
	<i>herunder hjelpesystemer som nødvendig belysning, kjøling og lignende.</i>
Kraftstasjoner klasse 2 skal ha stasjonsstrøm og nødstrøm tilsvarende som for øvrige stasjoner i klasse 2, se veiledning til krav 2.2.7.	Kraftstasjoner klasse 3 skal ha stasjonsstrøm og nødstrøm tilsvarende som for øvrige stasjoner i klasse 3, se veiledning til krav 3.2.9.
Separering av kabler i kraftstasjon	
2.3.9 Viktige kabler for driftskontroll og styre- og nødstrøm skal så langt som mulig fysisk separeres fra høyspentkabler.	3.3.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.
Kraftstasjoner klasse 2 skal ha separering av kabler tilsvarende som for klasse 2 stasjoner, se veiledning til krav 2.2.8.	Kraftstasjoner klasse 3 skal ha dublering og separering av kabler tilsvarende som for klasse 3 stasjoner, se veiledning til krav 3.2.10.

4.5 Oppstart av kraftstasjon på spenningsløst nett

klasse. 2	klasse. 3
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Oppstart av kraftstasjon på spenningsløst nett	
2.3.10 Minst ett aggregat skal normalt kunne starte på spenningsløst nett (svart nett).	3.3.9 Minst ett aggregat skal normalt kunne starte på spenningsløst nett (svart nett) og kunne drives separat (øydrift).
Alle kraftstasjoner i klasse 2 og 3 i ulike driftsområder skal kunne starte på spenningsløst (svart) nett for å kunne bygge opp sentral- og regionalnettet etter større utfall. Tilsvarende skal kraftstasjoner i klasse 3 i en ekstraordinær situasjon være stabile nok til å kunne drives separat og dermed holde nettet stabilt, i første omgang i et avgrenset område, men også ved langvarige avbrudd. Ut fra en lokal vurdering kan det også være aktuelt å ha ovennevnte beredskap også ved andre kraftverk. For krav til gjenopprettingsplan og operativ drift, viser vi til <i>forskrift om systemansvaret i kraftsystemet (fos)</i> og nettkoder for generatordrift.	

5 VEDLEGG 2 OG 3: - TILLEGG FOR DRIFTSKONTROLLSYSTEMER, KL. 2 OG 3

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
2.4 For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 2.1:	3.4 For driftskontrollsystemer gjelder følgende krav i tillegg til kravene i punkt 3.1:
Se funksjonsbaserte krav i kapittel 0 Se veiledning til kravene 2.4.1.1 til 2.4.1.7 og kravene 2.4.2.1 til 2.4.2.5	Se funksjonsbaserte krav i kapittel 0 Se veiledning til kravene 3.4.1.1 til 2.4.1.8 og kravene 3.4.2.1 til 3.4.2.4

5.1 Driftssentraler

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Driftssentraler (2.4.1 / 3.4.1)	
2.4.1.1 Driftssentraler skal plasseres i et bygg med god brann- og innbruddssikkerhet.	3.4.1.1 Driftssentraler skal plasseres i et solid bygg med god brann- og innbruddssikkerhet.
Brannsikring: Driftssentral bygges i egen branncelle med en brannmotstand på minst EI 60 REI 60 M for bygningsdeler hvor dette er relevant. Kabelgjennomføringer med mer. skal sikres tilsvarende. Det samme gjelder for vegger, kabelføringer med mer mellom de redundante delene av anlegget. Det bør installeres selvlukkende dører. Kabelgjennomføringer med mer. må ha tilsvarende brannsikring. Slukkemidler for raskt å slå ned en mindre brann må være tilgjengelig. Automatisk slukkeanlegg bør vurderes.	Brannsikring: Driftssentral bygges i egen branncelle med en brannmotstand på minst EI 60 og REI 60 M for bygningsdeler hvor dette er relevant. Brannmotstandstiden skal økes til 120 minutter dersom det ikke er installert automatisk slukkeutstyr. Ved dokumentert nærhet til permanent bemannet brannutrykningsenhet kan brannmotstandstiden reduseres, men ikke til mindre enn 60 min. Kabelgjennomføringer mm må ha tilsvarende brannsikring. Samme gjelder for vegger, kabelføringer mm. mellom de redundante delene av anlegget. Slukkemidler for raskt å slå ned en mindre brann må være tilgjengelig. Installering av automatisk slukkeutstyr må vurderes.
2.4.1.2 Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, varsling og rask reaksjon ved uønskede hendelser og handlinger.	3.4.1.2 Skal ha utstyr og prosedyrer for effektiv og pålitelig deteksjon, alarmer, verifikasjon og rask reaksjon mht. uønskede hendelser og handlinger.
Oppdagelse og reaksjon: Driftssentralen skal ha brann- og innbruddsalarm med effektiv varsling.	Oppdagelse og reaksjon: Driftssentralen skal ha brann og innbruddsalarm med automatisk brannalarmanlegg med detektorer i alle rom i den delen av bygget hvor driftssentralen med tilbehør

<i>klasse. 2</i>	<i>klasse. 3</i>
Dette gjelder i driftssentralens branncelle(r) og tilstøtende rom. Brannalarmen skal døgntkontinuerlig varsle driftspersonell, enten stedlig personell eller hjemmevakt, lokalt brannvesen eller annen bemannet driftssentral.	er plassert. Dette gjelder både i og utenfor driftssentralens branncelle(r), samt i etasjen over og under, oppganger, ventilasjonsjakter mm. Dette må sees i sammenheng med de ulike veggens og etasjeskilleres brannmotstand, og byggets brannsikkerhet forøvrig. Brannalarmen skal døgntkontinuerlig varsle driftspersonell, enten stedlig personell, hjemmevakt, lokalt brannvesen eller annen bemannet driftssentral. Om mulig bør brannvarsling også gå til lokal brann- og redningsetat. Selskapet må sørge for tilstrekkelig antall detektorer, sammenkoblet i et system, med forskjellige egenskaper for bedre verifikasjon (ioniske, optiske og varmesensitive).
<i>2.4.1.3 Skal være en egen fysisk sikret adgangskontrollert sone og utføres som egen branncelle med god brannsikkerhet og brannmotstand etter fastsatt norm.</i>	<i>3.4.1.3 Skal være egen fysisk sikret adgangskontrollerte sone(r) og utføres som egen branncelle(r) med høy brannsikkerhet og brannmotstand etter fastsatte normer.</i>
<i>Fysisk sonesikring:</i> For rom og bygningsdeler av vesentlig betydning for driftskontrollfunksjonene, det vil si hvor det er plassert viktig utstyr (datarom/ prosessmaskiner, sambandsrom/terminalutstyr og liknende), samt øvrige relevante rom (operatørrom, strømforsyning/ batterirom og liknende), utføres gulv, tak og utvendige vegger i minimum etter kravene i EN 1992. Er ikke dette mulig skal slike vegger vurderes forsterket med for eksempel stålplater eller solid kryssfiner. Forsterkningene skal sammen med det som forsterkes, ivareta krav både til fysisk styrke og brannsikring. Ventilasjonsåpninger og liknende sikres med gitter eller stålplater. Dører, låser, gitter med videre i utvendige vegger, bør utføres som sikkerhetsklasse 4 (minimum 3) etter EN (1627 med videre). Indre sonesikring utføres som sikkerhetsklasse 3 eller 4. Andre dører minimum EI 60, og utført i stål dersom de også skal tjene som sikring mot inntrengning. Selvlukking vurderes.	<i>Fysisk sonesikring:</i> For rom/bygningsdel av vesentlig betydning for driftskontrollfunksjonene, hvor det er plassert viktig utstyr (datarom/ prosessmaskiner, sambandsrom/ terminalutstyr og likende), samt øvrige relevante rom (operatørrom, strømforsyning/ batterirom og liknende) bør gulv, tak og utvendige vegger utføres i minimum 200 millimeter dobbeltarmert betong. Dimensjonene kan reduseres til minimumskravene i EN 1992. Er ikke dette mulig skal slike vegger med videre forsterkes med for eksempel 3 til 4 mm stålplater eller liknende med solid innfesting. Ventilasjonsåpninger og liknende sikres med gitter eller stålplater. Dører, låser, gitter med videre i utvendige vegger, bør utføres som sikkerhetsklasse 5 (minimum 4) etter EN (1627 med videre). På utsatte steder bør KD 10 eller tilsvarende vurderes. Indre sonesikring utføres som sikkerhetsklasse 4. Andre dører minimum EI 60, og utført i stål dersom de også skal tjene som sikring mot inntrengning. Selvlukking vurderes.

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>2.4.1.5 Operatørrom og andre bygningsdeler av vesentlig betydning for driftskontrollfunksjonene skal være normalt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.</i>	<i>3.4.1.4 Operatørrom og andre bygningsdeler av vesentlig betydning for driftskontrollfunksjonene skal være godt beskyttet etter fastsatte normer for hhv. fysisk sikring og brannmotstand.</i>
Operatørrom utstyres med sikkerhetsglass som minimum oppfyller klasse P6B (innbrudds-hemmende glass) etter EN 356. Slikt glass vil også være FG-godkjent. Størrelsen på vindusflatene bør begrenses mest mulig. For rom som ikke er fast arbeidsplass, kan et alternativ være å utstyre slike vinduer med solide stållemmer/ skodder eller liknende som enkelt kan trekkes for og låses. Rom for prosessanlegg, front-end, samband og liknende, bygges uten vinduer.	Operatørrom utstyres med sikkerhetsglass som minimum oppfyller klasse P7B (P8B vurderes) (innbrudds-hemmende glass) etter EN 356. Slikt glass vil også være FG- godkjent. Størrelsen på vindusflatene bør begrenses mest mulig. For rom som ikke er fast arbeidsplass, kan et alternativ være å utstyre slike vinduer med solide stållemmer/ skodder eller liknende som enkelt kan trekkes for og låses. Rom for prosessanlegg, front-end, samband og liknende bygges uten vinduer.
<i>2.4.1.4 Viktige komponenter og systemer skal ha redundans slik at én enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.</i>	<i>3.4.1.5 Alle komponenter og systemer skal utføres fullredundant med bl.a. dubberte og fysiske uavhengig prosessutstyr, føringsveier for strøm, signaler og sambandsutrustning, samt annen nødvendig utrustning, slik at en enkelt feil eller hendelse ikke kan slå ut vitale funksjoner.</i>
<i>Redundans:</i> Virksomheten må ha to SCADA-systemer der det ene kan ta over dersom det andre slutter å virke. Kommunikasjonslinjene må være dubberte. Den ene linjen kan være basert på offentlig ekom. Andre eksempler på dubberte systemer er dubberte batteribanker (UPS), sambandsløsninger – eget nødsamband og Nødnett. Listen er ikke uttømmende.	<i>Redundans:</i> Virksomheten må ha to SCADA-systemer der den ene kan ta over dersom det andre slutter å virke. Kommunikasjonslinjene må være adskilte og dubberte. Den ene linjen kan være basert på offentlig ekom. Andre eksempler på dubberte systemer er uavhengige dubberte batteribanker (UPS), sambandsløsninger – eget nødsamband og Nødnett. Listen er ikke uttømmende.
<i>2.4.1.6 Driftssentralens data-, sambands- og øvrige systemer som er nødvendige for driften av kraftsystemet, skal forsynes fra to uavhengige strømkurser. Dette inkluderer et nødstrømsanlegg med batteribank og avbruddsfri strømforsyning som skal en driftstid på minst seks timer. Dersom det ikke er installert permanent nødstrømsaggregat, skal et mobilt nødstrømsaggregat kunne kobles til og være tilgjengelig godt innenfor batterikapasiteten. Nødstrømsanlegget skal samlet sett ha automatisk start og gangtid på minst to døgn.</i>	<i>3.4.1.6 Skal ha et elektrisk og fysisk dubbert system for egen strømforsyning med nødstrøm som har tilstrekkelig kapasitet, kvalitet og utholdenhet. Herunder skal alle systemer som er nødvendige for driften forsynes fra to uavhengige og separerte strømkurser-/systemer. Dette skal også omfatte et nødstrømsystem som er dubbert med uavhengige batteribanker og avbruddsfri strømforsyning, og minimum har en samlet driftstid på minst seks timer. Det skal være installert et stasjonært nødstrømsaggregat med tilstrekkelig kapasitet og kvalitet, automatisk oppstart ved strønbrudd og minst tre døgn selvstendig driftstid. Et mobilt nødstrømsaggregat må raskt kunne kobles til dersom det stasjonære</i>

<i>klasse. 2</i>	<i>klasse. 3</i>
	<i>aggregatet skulle svikte. Nødstrømsystemet skal tåle de maksimale belastninger det kan bli utsatt for, herunder hjelpesystemer som nødvendig belysning, kjøling av nødvendig utrustning, og lignende.</i>
(Dette kravet er delvis likt krav 2.2.7.) Driftssentraler klasse 2 skal ha strømforsyning og nødstrøm tilsvarende som for klasse 2 stasjoner, se veiledning til krav 2.2.7.	(Dette kravet er likt krav 3.2.9) Driftssentraler klasse 3 skal ha strømforsyning og nødstrøm tilsvarende som for klasse 3 stasjoner, se veiledning til krav 3.2.9.
	<i>3.4.1.7 Dublering etter dette punkt skal så langt mulig utføres ved elektronisk, elektrisk og fysisk separering. Dersom dette ikke er mulig, skal fysisk seksjonering gjennomføres.</i>
	<i>Fysisk separering:</i> Det dublerte batterianlegget skal være plassert i separate brannceller. Batteribankene må ha opplegg for krysskobling, slik at hele batterikapasiteten kan utnyttes ved eventuelle feil i nødstrømsystemet.
<i>2.4.1.7 Skal ha et alternativt opplegg for utøvelse av alle viktige funksjoner i en ekstraordinær situasjon.</i>	<i>3.4.1.8 Skal ha et beredskapsrom og/ eller fysisk alternativ sted med opplegg for utøvelse av alle viktige funksjoner i en ekstraordinær situasjon.</i>
<i>Alternativ driftskontroll:</i> Driftskontrollsystemer i klasse 2 skal ut fra sin funksjon og betydning ha et alternativt opplegg for drift, ledelse og gjenoppretting i ekstraordinære situasjoner. Det alternative opplegget skal fungere på et annet sted enn den ordinære driftssentralen dersom den ordinære driftssentralen havarer, må evakueres eller blir ødelagt av for eksempel brann. Ved alternativ drift skal viktige funksjoner kunne ivaretas på en sikker og effektiv måte. Det kan gjøres ved hjelp av et forberedt alternativt sted der det rigges til med utstyr tilsvarende driftssentralen, eller ved at virksomheten har planer og ressurser for lokal betjening av aktuelle anlegg. Det er opp til den enkelte virksomheten å planlegge og etablere slik alternativ drift. Samband må være klart til bruk, og øvelser må gjennomføres for å kontrollere at opplegget virker og for å etablere og opprettholde kompetansen i forhold til en alternativ drift.	<i>Alternativ driftskontroll:</i> For driftskontrollsystemer i klasse 3 skal det være et etablert beredskapsrom med reserve driftskontrollsystem som kan tjene som nøddriftssentral dersom driftssentralen blir ødelagt ved for eksempel ødeleggelse eller havari i den ordinære driftssentralen. Beredskapsrommet med systemer skal være sikret og utstyrt tilsvarende driftssentralen. Beredskapsrommet skal være operativt på kort varsel. Virksomheten må derfor: • Ha forberedte planer for flytting fra driftssentral til beredskapsrom og oppstart drift fra beredskapsrommet • Ha oppdaterte utstyrlister, sikkerhetskopier av viktig informasjon og planer for alternativ drift • Ha kontroll på at sambandsveier, nødstrøm og øvrig nødvendig utstyr virker • På kort varsel kunne bemanne og utruste beredskapsrommet med de hjelpemidlene som trengs for å:

<i>klasse. 2</i>	<i>klasse. 3</i>
	○ kunne lede den delen av kraftforsyningen som virksomheten er ansvarlig for ○ ha løpende forbindelse med høyere og lavere ledd innenfor KBO ○ kommunisere med øvrige relevante etater (politi, statsforvaltere og andre)

5.2 Sambandsanlegg

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Sambandsanlegg (2.4.2 /3.4.2)	
2.4.2.1 Sambandsanlegg regnes normalt som en del av det driftskontrollsystem de inngår i.	(forskriften mangler tilsvarende krav for klasse 3, men kan legges til grunn samme ordlyd som i 2.4.2.1)
Fysisk sikring: Sambandsanlegg skal gis en tilfredsstillende fysisk sikring etter klasse og risiko for inntrenging, sabotasje, brann og andre former for ødeleggelse. Dette kan gjøres eksempelvis ved bruk av ikke brennbare materialer, brannslukningsanlegg/-utstyr, brann og innbruddsalarm. Vinduer skal unngås i alle sambandsanlegg, eventuelt skal de sikres med hærverks- eller innbruddshemmende glass, stållemmer, solide gitter eller liknende som låses eller boltes fra innsiden. Sikringsnivå tilsvarende som for driftssentral: Viktige eller utsatte sambandsanlegg i klasse 2 og 3 skal vurderes utført med relevante sikringstiltak som for driftssentral i samme klasse, slik at driftskontrollsystemet gis en helhetlig og balansert beskyttelse etter de ulike elementers betydning. I klasse 3 bør utvendige vegger i så fall bygges i 200 millimeter dobbeltarmert betong. Dimensjonene kan reduseres til minimumskravene i NS 3473 for vegger mellom rommene. Dører i utvendige vegger KD 10. Andre dører EI 60 (stål) eller bedre. Sambandsanlegg i klasse 2 og mindre utsatte anlegg i klasse 3 gis solid utførelse ved plassering i bygg av eksempelvis betongelementer, stålcontainer, samt ståldører.	
2.4.2.2 Anlegget skal planlegges og utføres slik at de tåler de maksimale påkjenninger de kan bli utsatt for.	3.4.2.1 Anlegget skal utføres så fysisk, elektrisk og elektronisk robust at det tåler påregnelig uvær og andre ytre påkjenninger, herunder atmosfæriske og elektromagnetiske forstyrrelser.
Ytre påkjenninger: Sambandsanlegg skal planlegges og utføres etter de maksimalbelastningene (uvær, ising med videre) de kan bli utsatt for. Dette gjelder særlig utsatte komponenter med tilhørende oppheng/føringer og festeanordninger som kabler, master, antenner, radiospeil, HF-sperrer med mer.	
2.4.2.3 Anlegget skal sikres mot uønskede hendelser og handlinger som innbrudd, hærverk, sabotasje og brann.	3.4.2.2 Utsatte anleggsdeler som kabler, master og antenner/radiospeil skal utføres særlig robuste, og bygg med adkomster som dører og vinduer må gis god sikring etter fastsatte normer for fysisk sikring.

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Sikring mot uønsket adgang og brann:</i> Antenneanlegg, master og kabelføringer sikres mot hærverk, sabotasje, uønsket adgang og brann. Dette omfatter bruk av ikke brennbare materialer, brannbeskyttelse av kabler, inngjerding av master, antenneanlegg, låsing av koplingsskap og tildekking/beskyttelse av kabeltrasé fram til disse. Strømforsyning og samband bør føres inn i anlegget gjennom jordkabler eller gis annen beskyttelse. Master beskyttes med klatrehindre.	
<i>2.4.2.4 Anlegg med god tilgjengelighet skal utstyres med nødstrøm med automatisk start og gangtid på minst to døgn. For vanskelig tilgjengelige anlegg skal inntil 14 døgn vurderes.</i>	<i>3.4.2.3 Anlegg med god tilgjengelighet året rundt skal utstyres med nødstrøm med automatisk start og gangtid på minst tre døgn, men for vanskelig tilgjengelige anlegg må dette etter forholdene økes til 30 døgn.</i>
Sambandsanlegg klasse 2 skal ha strømforsyning og nødstrøm tilsvarende som for klasse 2 stasjoner, se veiledning til kap. 3.4. Sambandsanlegg i lavlandet med god tilgjengelighet bør ha batterianlegg/ UPS med driftstid på 1 til 2 døgn og være forberedt for tilkobling til et tilgjengelig mobilt nødstrømsaggregat innen batteritiden slik at minstekravet samlet sett oppfylles. Vanskelig tilgjengelige sambandsanlegg (fjelltopper og liknende) utstyres vanligvis med batterianlegg med driftstid på 1 til 2 døgn eller mer, og stasjonært nødstrømsaggregat med gangtid inntil 14 døgn avhengig av muligheter for tilsyn/ vedlikehold og etterfylling av diesel. Alternativt kan stasjonen ha batterianlegg med driftstid på minst 2 til 3 døgn og være forberedt for tilkobling til mobilt nødstrømsaggregat. Dersom anlegget har god fysisk tilgjengelighet, kan kravene reduseres.	Sambandsanlegg klasse 3 skal ha strømforsyning og nødstrøm tilsvarende som for klasse 3 stasjoner, se veiledning til kap. 3.4. Sambandsanlegg i lavlandet med god tilgjengelighet skal ha batterianlegg/ UPS med driftstid på 3 døgn eller mer og nødstrømsaggregat eventuelt eller forberedt for tilkobling til et tilgjengelig mobilt aggregat. Viktige og vanskelig tilgjengelige sambandsanlegg (for eksempel radiolinjestasjoner (RL) på fjelltopper med mer) bør som et minimum utstyres med batterianlegg/ UPS med driftstid på 3 til 4 døgn og stasjonært nødstrømsaggregat med automatisk gangtid på 30 døgn. Dersom anlegget har gunstig beliggenhet med god fysisk tilgjengelighet året rundt, kan dette reduseres.
<i>2.4.2.5 Anlegget skal også oppfylle kravene som fremgår av kapittel 7.</i>	<i>3.4.2.4 Anlegget skal også oppfylle kravene som fremgår av kapittel 7.</i>
Kravet gjelder både for driftssentraler og sambandsanlegg.	

6 VEDLEGG 2 OG 3: KRAFTLEDNINGER KL. 2 OG 3

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
Kraftledninger	
<i>2.5.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessig betydning.</i>	<i>3.5.1 På grunnlag av risiko- og sårbarhetsanalyser skal selskapet sørge for å iverksette nødvendige sikrings- og beredskapstiltak ut fra stedlige forhold og samfunnsmessige betydning.</i>
<i>2.5.2 For kabler skal i tillegg viktige komponenter som endemuffer og skjøter beskyttes. Alternativt kan det anskaffes reservekomponenter som lagres på sikkert sted, og det skal være tilgang til reservekabel med mer etter § 4-4.</i>	<i>3.5.2 For kabler skal i tillegg viktige komponenter som endemuffer og skjøter beskyttes. Alternativt kan det anskaffes reservekomponenter som lagres på sikkert sted, og det skal anordnes reservekabel med nødvendig utstyr etter § 4-4.</i>
<i>2.5.3 Gjenoppretting av funksjonstap skal skje uten ugrunnet opphold.</i>	<i>3.5.3 Gjenoppretting av eventuelle funksjonstap skal skje så raskt som fysisk mulig.</i>
Kraftledninger etter disse bestemmelsene omfatter både luftledning og kabel i sjø og på land med tilhørende mufteanlegg. <i>Risikovurderinger:</i> En risikovurdering bør ta hensyn til stedlige forhold som for eksempel grunnforhold, adkomst og tilgjengelighet for linjerydding og feilretting mv. Risikovurderingen bør også ta hensyn til klimavariasjoner og ev. økt fare for naturgitte hendelser på grunn av klimaendringer. Kraftledningenes samfunnsmessige betydning kan f.eks. være kraftforsyning til helseinstitusjoner, offentlig beredskapsvirksomhet, mv. i henhold til egen oversikt over prioriterte kunder som virksomheten skal ha utarbeidet i en beredskaps- eller rasjoneringsplan etter § 6a og vedlegg 1 i <i>krafttrasjoneringsforskriften</i>. Kraftledninger kan være utsatt for værpåkjenninger som for eksempel sterk vind, ising, salting, atmosfæriske utladninger, trefall og lynnedslag. Mange ledninger er bygd i ras- og skredutsatte områder. Mindre ledninger kan være utsatt for skade fra nærstående vegetasjon i kombinasjon med sterk vind. Mekaniske og elektriske feil som følge av langvarig slitasje og elde forekommer også. Sabotasje kan heller ikke utelukkes. Bestemmelsene etter disse punktene - sammen med andre gjeldende krav og normer – skal bidra til å forhindre og motvirke at det oppstår feil og havarier som følge av disse og liknede uønskede hendelser. Vi forutsetter at regler i henholdsvis <i>forskrift om elektriske forsyningsanlegg</i> (fef) med veiledning, normer utgitt av NEK (Norsk Elektroteknisk Komité) og REN (Rasjonell Elektrisk Nettvirksomhet AS), følges så langt de er relevante og tilstrekkelige for å oppfylle forskriftens formål og bestemmelser. Vi vil særlig peke på ”Nasjonale Normative Forhold (NNA) for Norge” som er utarbeidet av NEK basert på EN og som er tatt inn i NEK 445 (siste utgave). Disse bør følges. I vurderingene og tiltakene som skal gjennomføres, må det tas hensyn til at klimabelastningene kan øke betydelig i årene som	

kommer. Videre skal det fullt ut tas hensyn til ulike kombinerte belastninger som følge av for eksempel vind og ising.

Trasevalg og krav til trasé

Ved planlegging av nye anlegg bør det vektlegges å finne traseer og løsninger som ikke gir risiko for skader og havari som følge av ras/skred, flom, kollisjoner e.l. Dersom ledningen må passere utsatte områder (for eksempel der det er fare for ras og skred) bør parallelle master unngås, om det ikke kan gjøres tiltak som ekstra forstreknings, skredavvisere og liknende.

Master, oppheng, ledere og liknende

Forskriftens krav oppfylles ikke dersom man anvender svake/mindre stabile konstruksjoner. Slike konstruksjoner kan for eksempel være høyspentmaster med kun én bærende trestolpe i områder med krevende klima eller som hjørnestolper. Unntak gjelder for midlertidige reparasjoner eller spesialkonstruerte reservemaster. Av hensyn til blant annet estetikk og plass har flere land utviklet og dels tatt i bruk ukonvensjonelle stålmaster og liknende for høyere spenninger. Før slike eventuelt tas i bruk i Norge i større omfang, bør det både ut fra teoretiske beregninger og praktisk erfaringer, kunne dokumenteres at disse tåler de belastningene de kan bli utsatt for i Norge. Ellers viser vi til veiledningen til *forskrift om elektriske forsyningsanlegg* (fef) kapittel 6 Høyspenningsluftlinjer.

Elektrisk og mekanisk dimensjonering

Kraftledningen skal til enhver tid tåle den spenningen og den overføringsevnen som er gitt i konsesjonen og er innrapportert til og vedtatt av systemansvarlig (eventuelt NVE) etter bestemmelser om overføringsgrenser i forskrift om systemansvaret i kraftsystemet (FoS). For krav til isolasjon med videre for luftledning, se veiledningen til fef kapittel 4 Høyspenningsluftlinjer.

7 VEDLEGG 2: FJERNVARMEANLEGG, KL. 2

<i>klasse. 2</i>	<i>klasse. 3</i>
<i>Dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet i punkt 2.2 til 2.5 for klasse 2 og i punkt 3.2 til 3.6 for klasse 3</i>	
<i>Fjernvarmeanlegg</i>	
2.6 <i>For fjernvarmeanlegg gjelder følgende krav i tillegg til kravene i punkt 2.1:</i>	
Se funksjonsbaserte krav i kapittel 0.	Ingen fjernvarmeanlegg er klassifisert i klasse 3.
2.6.1 <i>Beredskapsmyndigheten kan fastsette særlige krav til sikring av fjernvarmeanlegg.</i>	
NVE har utarbeidet en egen veiledning om fjernvarmeberedskap, se <u>NVE-veileder nr. 5-2015</u> .	

8 VEDLEGG 4 NORMER OG STANDARDER

8.1 Relevante normer og standarder



Vedlegg 4: Henvisning til normer og standarder i forskriften

Alle KBO-enheter skal dokumentere hvilke normer som er brukt når dette er relevant for å oppfylle denne forskrift. De normer det henvises til er gjeldende Norsk standard (NS) basert på likeverdig europeisk norm (EN):

NS-EN 13501 Brannklassifisering av byggevarer og bygningsdeler

NS-EN 1627 Inngangsdører, vinduer, påhengsvegger, gitter og skodder – Innbruddssikkerhet – Krav og klassifisering

NS-EN 1303 Bygningsbeslag – Låssylindere – Krav og prøvingsmetoder

NS-EN 12209 Bygningsbeslag – Låser og fallelåser – Mekanisk betjente låser, fallelåser og beskyttelseskåper – Krav og prøvingsmetoder

NS-EN 12320 Bygningsbeslag – Hengelåser og hengelåsbeslag – Krav og prøvingsmetoder

NS-EN 356 Bygningsglass – Sikkerhetsruter – Prøving og klassifisering av motstand mot innbrudd og hærverk

NS-EN 1990 Eurokode – Grunnlag for prosjektering av konstruksjoner

NS-EN 1992 Eurokode 2: Prosjektering av betongkonstruksjoner – Del 1-1: Allmenne regler og regler for bygninger

Andre normer kan for eksempel være utarbeidet av Forsikringsselskapenes Godkjennelsesnevnd (FG).

I tilfeller hvor normer ikke kan følges, eksempelvis fordi det ikke finnes relevante godkjente produkter eller på grunn av andre hensyn, skal det dokumenteres at valgt løsning oppfyller forskriftens krav gjennom et likeverdig sikringsnivå.

Vedlegg 4 viser en oversikt over hvilke normer og standarder som er relevante. Hensikten med bruk av normer og standarder, er at man på en enkel og dokumenterbar måte kan få levert produkter som oppfyller kravene og anbefalingene til funksjon og sikringsnivå.

I bestemmelsen om sikringsnivå henviser NVE til gjeldende normer om brannvern, konstruksjoner og beskyttelse mot inntrengning, først og fremst til europeiske normer (EN) som er antatt som norsk standard NS-EN. Også svensk og internordisk standard er en del brukt innen de samme tema. De nordiske forsikringsforbundene har innen blant annet innbruddsikring utarbeidet en ”sammenligningsnøkkel”. Denne med forklaring til normer for sikring og sikkerhet finnes på nettsidene til Forsikringsselskapenes Godkjennelsesnevnd (FG). Også Direktoratet for samfunnssikkerhet og beredskap henviser til ulike relevante normer i sitt regelverk og publikasjoner.

Formålet med henvisningen til normer og standarder er å vise hvor nivået skal ligge for ulike produkter.

Kategorier av sikringsnivå i standarder, vs. sikringsnivå i kbf



Sikringskravene som er gitt av kraftberedskapsforskriften (kbf) har tre klasser, i dette eksempelet kalt beredskapsklasser for å gjøre det tydeligere:

- Krav til sikring av anlegg i beredskapsklasse 1 er gitt av kbf § 5-4
«Sikringstiltak for klasse 1»: Anlegget skal utføres med normalt sikringsnivå som nærmere angitt i vedlegg 1
- Krav til sikring av anlegg i beredskapsklasse 2 er gitt av kbf § 5-5
«Sikringstiltak for klasse 2»: Anlegget skal utføres etter middels høye krav til sikring, som nærmere angitt i vedlegg 2
- Krav til sikring av anlegg i beredskapsklasse 3 er gitt av kbf § 5-6
«Sikringstiltak for klasse 3»: Anlegget skal utføres etter høye krav til sikring, som nærmere angitt i vedlegg 3

Vedleggene som disse henviser til er vedleggene til forskriften, ikke veiledningen.

For krav til sikring mot innbrudd og inntrengning – er relevante normer blant annet EN 1627, EN 1303, EN 12209 og EN12320. Se også forskriftens vedlegg 4 som gir en liste over relevante standarder. Disse har seks sikringsklasser på en stigende skala fra en til seks. Også kalt motstandsklasser - resistance class (RC) eller grade.

I avsnittet nedenfor, «Sammenhengen mellom sikringsnivå i kbf og sikringklasser i utvalgte europeiske standarder» er det oppstilt en oversikt over hva vi anser som normalt, middels, godt og høyt sikringsnivå i henhold til kravene i kbf vedlegg 1, 2 og 3.

Vi kan som hovedregel si at:

- Normalt sikringsnivå i henhold til beredskapsklasse 1 og vedlegg 1 er tilfredsstilt ved å velge minst sikringsklasse 2 fra standardene
- Middels eller «god» sikringsnivå i henhold til beredskapsklasse 2 og vedlegg 2 er tilfredsstilt ved å velge minst sikringsklasse 3 eller 4 fra standardene
- Høyt sikringsnivå i henhold til beredskapsklasse 3 og vedlegg 3 er tilfredsstilt ved å velge minst sikringsklasse 5 eller 6 fra standardene

Valg av sikringsklasse fra standardene alene er ikke tilstrekkelig for å oppnå tilfredsstillende beredskapssikringsnivå ved planlegging, prosjektering og bygging. Bygging, vesentlige endringer eller utvidelser skal alltid utføres på bakgrunn av risikovurderinger, se kbf §§ 2.3, 5-3 og 5-8 De funksjonsbaserte kravene skal utgjøre en balansert helhet, se kravene 3.1.1 til 2.1.4 i kbf vedlegg 2 og 3.1.1 til 3.1.4 i vedlegg 3.

8.2 Sammenhengen mellom sikringsnivå i kbf og sikringklasser i utvalgte europeiske standarder

Sammenhenger mellom sikringsnivå i kbf kapittel 5 og sikringklasser etter europeiske normer (NS-EN) for ulike elementer i en balansert sikring Sikringsklasser (mot innbrudd ol.) hvor "motstandsstyrken" er kvantifisert (testkriterier) i form av innbruddstider for ulike verktøy og angrepsmetoder Dette er så koblet videre til andre elementer i en helhetlig skallsikring og de ulike standarder og klasser som finnes for disse.

NB! Dette er bare eksempler mht. av de mest relevante normer og klasser. For veiledende krav etter kbf § 5-4 til § 5-6 Sikringstiltak (etter klasse)

kbf sikringsnivå	Låser m/beslag	Hengelåser	Dører, gitter mv.	Vegger ol.			Glass (gml. standard i parentes)		Låser m/beslag
Vedlegg 1 til 3	EN 1303, 12209	EN 12320	EN 1627	tykkelse	kvalitet	armering	EN 356	ca. tykkelse i mm	FG klasse
Normal	sikringsklasse 2 (helst 3)			helstein	murvegg	armert	Hærverkshemmende (laminert) P 5A (A3+) 10		FG 2
				armert betong:			Innbruddshemmende (laminert)		
Middels	sikringsklasse 3			80 mm	B 30	K 189	P6B (B1) 12		FG 2 eller 3
God	sikringsklasse 4			120 mm	B 30	K 257	P7B (B2) 15		FG 3 eller 4
Høy	sikringsklasse 5			150 mm	B 35	K 355	P8B (B3) 18 - 20		FG 4 eller 5
	sikringsklasse 6			200 mm	B 35	K 355	EN 1063		
Eventuelt kraftigere innbruddsikring etter bl.a. EN 1143				osv. j.f. konstruksjonskrav etter EN 1990 og EN 1992			Skuddhemmende (multilaminert) BR 2 (C1) c) 19 til 25 d) (Tidligere "RSK" krav operatørrom)		Sikring mot dirking: minimum FG 3
							d) glasstykkelse avhenger av krav til sikring mot splinter/avskalling på innsid		
De overnvente sikringklasser (eng: "grade") er å anse som minimum				[Skala skuddsikkert fortsetter opp til BR 7 og videre i SG for tyngre våpen]					
Sikringsklasse 1 godtas ikke for anlegg klassifisert etter bfe.				Denne kolonnen gir kun tilnærmet ekvivalente klasser					
Normal er mao. her å anse som et minimum									

Merk! Disse klassene/kravene omfatter i utgangspunktet ikke brannsikring. Dette inkludert rømningsveier ol. må vurderes særskilt. Generelt bør yttervegger og seksjonerende vegger være i brannklasse REI 60 eller bedre, dører mv. i EI 60 eller bedre. De dimensjoner, kvaliteter mv. som er angitt i denne tabell tar kun hensyn til sikringsmessige krav. De bygningstekniske mv. krav til konstruksjonen som sådan må beregnes og utføres etter gjeldende regler/normer

9 TILLEGG OM BEREDSKAPSRØM

Dette tillegg er et uredigert utdrag fra ~~veileder nr. 1-2013~~ til beredskapsforskriften, side 118-119 og vedlegg 13.

Ved prosjektering av beredskapsrom benyttes kravene til tilfluktsrom etter *forskrift om tilfluktsrom*. I tillegg skal kravene i etterfølgende tabell være oppfylt.

Plassbehov	Gassluse	Ventilasjon
Min. 2 m ² / per person.	I alle beredskapsrom. Innvendige mål minimum: L x B = 2,5 x 1,5 m	Normalventilasjon: Min. 20 m ³ /time & person Filterventilasjon: Min. 10 m ³ /time & person.

Nødstrømsforsyning med batterier eller dieselaggregat skal vurderes i hvert enkelte tilfelle, se kravene til nødstrøm for driftssentral i klasse 3 i vedlegg 3 til bfe, punkt 3.4.1.6. Enheten må foreta sluttkontroll av tetthet, overtrykk, installasjon og andre relevante forhold.

Det skal foreligge oppdaterte utstyrlister, og planer for utstyr som skal bli tilført.

For utstyrliste, se vedlegg 13 til veiledningen.

9.1 Drift og vedlikehold

Det skal være utpekt personer som er ansvarlige for drift og vedlikehold av beredskapsrommene. Den som er ansvarlig for vedlikehold, skal ved regelmessige inspeksjoner sørge for at rommenes verneevne ikke forringes. Slitte eller defekte komponenter skal utbedres, eller skiftes ut. Det skal foreligge en oversikt over rommenes inventar og utstyr. Forskrifter og bruksanvisning med norsk tekst for vifter, aggregater, batterier og annet, skal være oppslått i nærheten av objektene.

For kontroll av temperatur og fuktighet skal termometre og hygrometre plasseres på hensiktsmessige steder i anlegget. Grunntemperaturen bør ligge på ca. 15° C og den relative fuktigheten bør ikke være over 50 - 60 %.

Beredskapsrommene skal kontrolleres ved rutinemessige inspeksjoner. For anlegg i dagen, bør kontrollen utføres hvert kvartal, for fjellanlegg hver 14. dag. Inspeksjonene skal protokollføres med angivelse av tidspunkt, resultat av inspeksjonen og hva som er gjort for å rette eventuelle feil og/eller mangler.

Se vedlegg 13 til veiledningen for liste over hva som skal kontrolleres ved de rutinemessige inspeksjonene.

9.2 Kontroll

I tillegg til de nevnte inspeksjonene skal alle beredskapsrom kontrolleres minimum én gang hvert år.

Når det ved beredskap beordres klargjøring av beredskapsrom, skal enheten gjennomføre fullstendig vedlikeholdsinspeksjon. Blant annet skal enheten funksjonsprøve og kontrollere at tekniske installasjoner virker slik det er forutsatt, og straks utbedre eventuelle mangler.

Se vedlegg 13 til veiledningen for sjekkliste for disse kontrollene.

9.3 Eksisterende beredskapsrom

Nyere beredskapsrom som er etablert ifølge BfK (2002), skal som hovedregel beholdes.

Eldre beredskapsrom ble tidligere også benevnt beskyttende rom eller ”kommando- eller alarmplasser”. Disse ble i sin tid pålagt av NVE eller tidligere KSFN - Kraftforsyningens sivilforsvarsnemnd. De kan også være kombinert med tilfluktsrom etter Sivilforsvarets krav.

Kommandoplasser var tilfluktsromsliknende (beskyttende)rom/områder i administrasjonsbygg og liknende, hvor ledelse og driftspersonell kunne søke tilflukt ved krigshandlinger og liknende – der de også kunne utøve ledelsesfunksjoner.

Alarmplasser var mindre - ofte enklere utstyrte - tilfluktsrom gjerne i forbindelse med kraftanlegg (stasjoner) hvor personell (driftspersonell, montører og liknende) på samme måte kunne søke tilflukt/beskyttelse. De må ikke forveksles med redningsrom, men kan også ha en kombinert funksjon med slike.

Kommando- og alarmplasser var fram til 1990- tallet pålagt gjennom enkeltvedtak. NVE har oversikter for hvert enkelte selskap (enhet i KBO) om pålegg for anordning og kontroll av disse. Det fantes også et detaljert regelverk gitt sist (1997) ved henholdsvis ”RSK” - Retningslinjer for sikring av kraftforsyningsanlegg” (kap. 14 *Beskyttende rom*) og ”BHK” – Beredskapshåndbok for kraftforsyningen”. I nyere tid var dette regulert i BfK § 6-4 *punkt f. Beredskapsrom*, og er knyttet opp mot driftskontrollfunksjonene.

Selv om mange av de eksisterende eldre beredskapsrommene ikke hadde blitt pålagt i dag, skal likevel tidligere tiders pålagte og utførte sikringstiltak opprettholdes - gitt at de fremdeles har eller kan få en funksjon ved beredskap, ikke er for kostbare å vedlikeholde, og ikke står i veien for en hensiktsmessig utvikling (modernisering, utvidelser) av bygg og anlegg.

På en noen steder har ikke lenger nevnte ”kommando- og alarmplasser” noen vesentlig funksjon. Dette fordi det enten ikke finnes noe stedlig personell, eller de er i en slik tilstand at de neppe vil ha den tiltenkte beskyttende effekt, eller at vedkommende stasjon neppe kan tenkes å bli utsatt for relevant risiko.

Dersom et slikt beredskapsrom:

- ikke fyller noen funksjon etter denne forskriften,
- ikke også er tilfluktsrom etter Sivilforsvarets krav,
- ikke fyller noen funksjon som redningsrom for personell (ved brann o.l.),
- ikke i det øvrige kan antas å ha eller få noen vesentlig beredskapsmessig betydning for vedkommende enhet – jf. lokal ROS-analyser og beredskapsplaner,

kan de nedlegges eller omdisponeres dersom vedkommende KBO-enhet ser behov for det.

For å få dokumentert og utkvittert gamle vedtak, sendes en kort melding (oversikt) til NVE om hvilke steder dette eventuelt gjelder.

9.4 Beredskapsrom – utstyr, drift, vedlikehold og kontroll

Utstysliste for beredskapsrom

Følgende utstyr bør være i eller i nærheten (raskt tilgjengelig) av beredskapsrom:

- Sambandsutstyr
- Radio
- Termometer og hygrometer
- Håndlykter
- Brannslukningsutstyr - apparat (pulver) og/eller brannslange
- Førstehjelpsutstyr, stasjonær førstehjelpsenhet
- Sykebåre med 2 ulltepper og annet mobilt førstehjelpsutstyr • Vannbeholdere/plastkanner med tappekran (20 liter per person, min. 100 liter bærbart)
- Toalett, vaske- og rengjøringsutstyr
- Bord og stoler
- Senger/hvilestoler
- Håndverktøy
- Utbrytningsverktøy bestående av spett, slegge (med reserveskaft), krafse, meisel
- Klosser for underlag for åpning av dører
- Reserve lyspærer, sikringer, batterier med mer
- Reservedeler for nødstrømsaggregat (viftereim, pakninger og liknende)
- Personlig utstyr
- Annet enheten finner relevant

Det skal foreligge oppdaterte utstyslister, og planer for utstyr som skal bli tilført.

Drift og vedlikehold

Ved de rutinemessige inspeksjonene skal følgende kontrolleres:

Bygningsteknisk:

- Dører, luker og porter
- Vannlekkasjer
- Skader på betong
- Rustangrep på stålkonstruksjoner
- Fuktighetsangrep på trekonstruksjoner

Ventilasjon

- Ventilasjonsanlegg med prøvekjøring av ventilasjonsaggregat. Det kontrolleres at viftene for fredsventilasjon er i orden og at det ikke er ulyder i lagre, motor, vifter, med mer
- Ventiler av alle slag kontrolleres. Om nødvendig foretas demontering og rengjøring og innsetting av alle bevegelige deler og anleggsflater med silikonholdig olje

10 REFERANSER

<i>Sikringshåndboka</i>	Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje, spionasje og annen kriminalitet. (Forsvarsbygg)
<i>Fjernvarmeberedskap</i>	Veiledning om fjernvarmeberedskap, se <i>NVE veileder nr. 5-2015</i>
<i>REN-blad 7683</i>	Områdesikring av transformatorstasjon
<i>REN-blad 7685</i>	Skallsikring av transformatorstasjon
<i>REN-blad 7007</i>	Lokal strømforsyning til transformatorstasjon
<i>NVE rapport 2/2009</i>	Tiltak for å redusere sannsynligheten for at et område er strømløst over lang tid, Regelverksprosjekt mellom NVE, DSB og Statnett http://publikasjoner.nve.no/rapport/2009/rapport2009_02.pdf
<i>Difi rapport 4/2009</i>	Sikker levering av elektrisk kraft - Grensesnittet mellom Direktorat for samfunnssikkerhet og beredskap og Norges vassdrags- og energidirektorat - https://evalueringsportalen.no/evaluering/sikker-levering-av-elektrisk-kraft-grensesnittet-mellom-direktorat-for-samfunnssikkerhet-og-beredskap-og-norges-vassdrags-og-energidirektorat/Difirapp.pdf/@@inline
<i>Referanse?</i>	Overlappprosjektet mellom NVE og DSB i 2011 Behandlet i tilsynsseminar NVE, DSB og energibransjen 27. september 2011 (NVE-sak 201103556)
<i>NVE ekstern rapport</i>	NVE Ekstern Rapport nr 15/2021 Tiltak for å motvirke konsekvenser og håndtere risiko knyttet til geomagnetisk induisert strøm i kraftnettet (SINTEF)



Krysskoplinger til andre paragrafer i denne forskriften

- [§ 2-3 Risikovurdering](#)
- [§ 2-4 Beredskapsplanlegging](#)
- [§ 4-1 Reparasjonsberedskap](#)
- [§ 5-3 Sikring av klassifiserte anlegg](#)
- [§ 5-8 Vurdering](#)

Koplinger til annet regelverk

- [Forskrift om systemansvaret i kraftsystemet](#)
- [Krafrasjoneringsforskriften](#)
- [Forskrift om elektriske forsyningsanlegg](#)