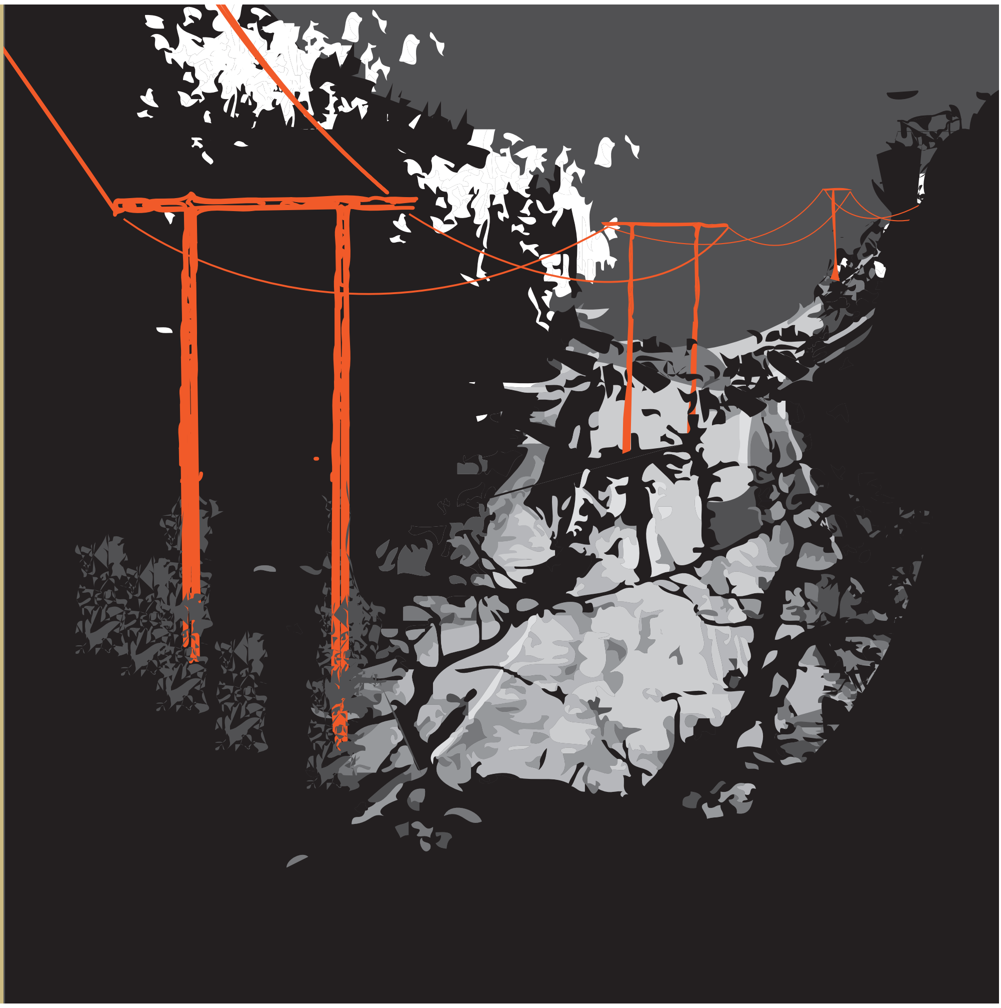
NVE

Veiledning til forskrift om beredskap i kraftforsyningen

1
2011



VEILEDER

Veiledning til forskrift om beredskap i kraftforsyningen

Norges vassdrags- og energidirektorat
2011

Veileder nr. 1-2011

Veiledning til forskrift om beredskap i kraftforsyningen

Utgitt av: Norges vassdrags- og energidirektorat

Redaktør: Arthur Gjengstø og Rikke C. Arnulf.
Forfatter: Frank Skapalen, Helge Ulsberg, Roger Steen, Rikke C. Arnulf og Truls Sønsteby.
ISSN: 1501-0678

Trykk: NVEs hustrykkeri
Opplag: Kun på nett
Forsidefoto:

Sammendrag:

Emneord:

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

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

Mars 2011

Innhold

Forord

Samfunnet er avhengig av stabile leveranser av elektrisitet og fjernvarme. Kraftforsyning er en av samfunnets aller viktigste infrastrukturer, og dette forplikter.

Gjennom forskrift om beredskap i kraftforsyningen stilles det klare krav til alle enheter innen kraftforsyningens beredskapsorganisasjon (KBO) om å arbeide systematisk med tiltak for å forebygge og håndtere ekstraordinære hendelser som kan skade eller hindre produksjon, overføring eller fordeling av elektrisk energi eller fjernvarme.

Viktigste målgruppe for denne veilederen er de enheter som forestår produksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme etter energiloven, og inngår i Kraftforsyningens beredskapsorganisasjon. Blant disse inngår også eiere av termisk kraftproduksjon, gasskraft, vindkraft og for fjernvarme, både varmesentraler og rørnett.

I denne versjonen av veilederen er det foretatt en total gjennomgang av hele dokumentet. Det har vært lagt vekt på å gjøre veiledningen tydeligere og mer konkret. Det har også vært lagt vekt på å innhente råd og synspunkter fra bransjen, og vi er glad for alle de innspill vi har fått i dette arbeidet.

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

Oslo, mars 2011

Agnar Aas

Vassdrags- og energidirektør

Om forskrift om beredskap i kraftforsyningen og veiledningen

Hjemmel: Fastsatt av Norges vassdrags- og energidirektorat 16. desember 2002 med hjemmel i Kronprinsreg.res. av 7. desember 1990 nr. 959 § 9-1 og lov av 29. juni 1990 nr. 50 om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) § 10-6. Endringer: Endret ved forskrifter 14. desember 2006 nr. 1413, 15. juni 2010 nr. 835.

Hensikten med forskrift om beredskap i kraftforsyningen (beredskapsforskriften, BfK) er å stille minimumskrav til alle enheter i kraftforsyningens beredskapsorganisasjon (KBO), slik at enhetene er i stand til å forebygge og håndtere ekstraordinære hendelser som kan skade eller hindre produksjon, overføring eller fordeling av elektrisk kraft og fjernvarme.

I hovedsak setter forskriften krav til funksjonelle, overordnede mål. Forskriften inneholder også på noen områder detaljerte krav. Veiledningen utdyper og forklarer forskriftsteksten.

Forskrift om beredskap i kraftforsyningen med veiledning gjelder også for fjernvarmeanlegg. Enkelte krav i § 5-5 lar seg imidlertid ikke oppfylle uten videre for denne typen anlegg, og NVE vil se nærmere på dette i et eget prosjekt.

Utforming av veiledningen

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

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

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

Hvis enheten velger en annen løsning enn den som er beskrevet i veiledningen, eller gjennomført risiko- og sårbarhetsanalyser tilsier at det er behov for en løsning med høyere ytelsesnivå, må det kunne dokumenteres at valgt løsning er like bra eller bedre enn den som er beskrevet i veiledningen. ROS-analyser kan med andre ord ikke gi grunnlag for å anvende løsninger som innebærer et lavere ytelsesnivå enn beskrevet i veilederen.

Forskriftsteksten er innrammet slik at den skiller seg fra tekstene forøvrig. Den etterfølgende teksten er veiledning som gir utfyllende kommentarer til hvordan forskriftens bestemmelser kan oppfylles. Grå tekstbokser gir eksempler.

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

Veiledningen må leses som et helhetlig dokument. Eksempelvis ligger ikke alle kravene til driftskontrollsystemer under § 6-4 Særlige krav til driftskontrollsystemer, men man må blant annet også se på § 5-5 Sikringsnivå. Kravet til ROS-analyser omfatter mange bestemmelser i forskriften, blant annet skal man gjennomføre ROS-analyse for samband og transportberedskap.

Enkelte krav til utførelse i forbindelse med §§ 5-5 Sikringsnivå og 6-4 Særlige krav til driftskontrollsystemer er sensitiv informasjon og underlagt taushetsplikt. Den taushetsbelagte delen av veiledningen kan fås etter behov, ved henvendelse til NVE.

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

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

Kap 1 Innledende bestemmelser

Bestemmelsene i kapittel 1 fastsetter hvordan KBO-enhetene skal arbeide systematisk med beredskap.
NVE anbefaler herunder at enheten utarbeider konkrete mål for beredskapsarbeidet.

§1-1 Beredskapskonsept

Alle enheter i Kraftforsyningens beredskapsorganisasjon (KBO) skal implementere et helhetlig beredskapskonsept. Konseptet skal optimalisere forebygging og håndtering av alle ekstraordinære situasjoner som kan skade eller hindre produksjon, overføring og fordeling av elektrisk kraft. Konseptet skal integreres i ordinær aktivitet.

Beredskapskonseptet skal bestå av følgende hovedfaser:

a) Analysere trusler og risikoer,

b) gjennomføre forebyggende tiltak,

c) planlegge og organisere for å kunne håndtere ekstraordinære situasjoner,

d) håndtere ekstraordinære situasjoner og gjenopprette funksjonalitet, og

e) evaluere øvelser og hendelser.

Veiledning

Alle enheter som inngår i KBO skal ha et beredskapskonsept. Enhetene skal arbeide systematisk med ROS-analyser for ekstraordinære situasjoner og følge opp dette med forebyggende og beredskapsmessige tiltak. Det forventes at arbeidet med beredskap er klart forankret i organisasjonen og enhetens ledelse. Dette kravet gjelder for enheter som driver produksjon, overføring og distribusjon av elektrisk kraft og fjernvarme, se også § 2-2 Organisering.

1.1.1 Et helhetlig beredskapskonsept

Arbeidet med et helhetlig konsept skal ha som mål å sikre god beredskap og forsyningssikkerhet. I henhold til beredskapsforskriften skal konseptet være helhetlig, hvilket vil si at enheten skal se på og vurdere alle forhold som kan redusere eller true egen evne til å oppfylle forskriftens krav. Med helhetlig menes videre at enheten skal kunne dokumentere at alle deler av beredskapsarbeidet er ivaretatt, at prosessen er forankret i ledelsen og at arbeidet er lagt opp til å være kontinuerlig:

Enhetens ledelse plikter å sikre denne helheten ved å sørge for at det er sammenheng mellom alle ledd i beredskapsarbeidet, listet som a-e i denne bestemmelsen.

Kontinuitet i arbeidet gjør det mulig for enhetene å løpende ta hensyn til nye utfordringer. Enheten skal fortløpende identifisere uønskede hendelser som kan hindre forsyningssikkerheten. Dette gjøres gjennom ROS-analyser. Med utgangspunkt i disse analysene skal enheten kartlegge og implementere forebyggende og skadereduserende tiltak. Etter gjennomførte ROS-analyser må enheten lage en beredskapsplan for å håndtere restrisiko og annet etter § 1-4 Beredskapsplan. Vurderingen av hva som skal med i beredskapsplanen bør komme til uttrykk gjennom en beredskapsanalyse, hvor enheten definerer egne krav til beredskap; dimensjonering av beredskapsressurser (både organisatoriske og materielle) og responstid utover pliktene gitt i beredskapsforskriften. Når hendelser inntreffer, settes øvet planverk ut i livet. Når planverket har vært i bruk, enten gjennom øvelser eller reelle hendelser, skal det evalueres og være utgangspunkt for nye ROS-analyser og oppdateringer av eksisterende ROS-analyser.

1.1.2 Ekstraordinære hendelser

Arbeidet med beredskapskonseptet skal omfatte hele bredden av ekstraordinære hendelser, det vil si naturgitte forhold, teknisk svikt eller tilsiktede ødeleggelser, og disse skal beskrives. Hva som er ekstraordinært, er ofte situasjonsbetinget, men i grove trekk kan man forklare begrepet med en uønsket hendelse som går utover de feilsituasjoner som selskapet håndterer i det daglige. Under arbeidet med å identifisere uønskede hendelser er det viktig å skille mellom årsak (eks: storm/uvær) og uønsket hendelse (eks: havarert mast).

I tillegg til å kartlegge mulige hendelser som kan true kraftforsyningen, plikter enheten å kartlegge sårbarheter. Enheten må vurdere om pålagte beredskapstiltak vil kunne fungere under press, eksempelvis ved redusert bemanning og/eller langvarige ekstraordinære hendelser. Ut fra kartlagte sårbarheter bør det vurderes hvorvidt det vil være nødvendig med flere tiltak utover den pålagte grunnsikringen.

1.1.3 Forebygging og håndtering av ekstraordinære situasjoner

At enheten skal optimalisere forebygging og evnen til håndtering av ekstraordinære situasjoner, betyr at enheten aktivt og jevnlig skal gjøre tilpasninger i sitt beredskapskonsept som gjør at enheten stadig blir bedre til å forebygge og håndtere ekstraordinære situasjoner.

1.1.4 Integreres i ordinær aktivitet

At konseptet skal integreres i ordinær aktivitet betyr at beredskapsarbeidet skal være forankret i virksomhetsstyringen, inngå i daglige rutiner og være kjent av alle aktuelle medarbeidere, deriblant ledelsen og enhetens styre.

Enheten må ta for seg alle kravene i forskriften og avgjøre hvordan disse på best mulig måte kan integreres med enhetens øvrige kvalitetssystemer og rutiner. Forskriftsteksten kan brukes som en sjekkliste.

Eksempler på at beredskapskonseptet er integrert i ordinær aktivitet:

- Relevante personer (ledelse og fagspesialister) i organisasjonen bidrar under planlegging og organisering for å kunne håndtere ekstraordinære situasjoner
- Enhetens budsjett tar høyde for utgifter til beredskapsaktiviteter
- Beredskapsmateriell tas med i ordinære kontroll- og vedlikeholdsrutiner

§1-2 Kvalitetssystem

Alle enheter i KBO skal ha et kvalitetssystem som dokumenterer at kravene i denne forskriften er oppfylt. Systemet skal inneholde opplysninger og dokumentasjon som er nødvendig for å gjennomføre tilsyn. Systemet skal gjenspeile faktisk tilstand, og dette skal kunne kontrolleres

Veiledning

Det skal kunne dokumenteres at alle krav i beredskapsforskriften er oppfylt. Kvalitetssystemet skal være et virkemiddel for å sikre og utvikle kvalitet i beredskapsarbeidet. Det vises også til energilovforskriften § 8-7 der det heter at det skal etableres internkontroll for kraftforsyningsberedskap.

Det er en forutsetning for oppfyllelse av bestemmelsene i §1-2 at beredskapsforskriften er godt kjent hos alle i enheten.

Kvalitetssystemet skal vise at:

- Enheten når sine fastsatte mål for beredskapsarbeidet.
- Enhetens beredskapsstatus er i samsvar med beredskapsforskriftens krav.
- Enheten gjør korrigerende tiltak dersom det avdekkes avvik.
- Enheten sørger for nødvendig intern opplæring i beredskapsforskriftens krav.

Enhetens kvalitetssystem bør som minimum:

- Ivareta alle krav i beredskapsforskriften og eget beredskapskonsept.
- På en enkel og forståelig måte vise godkjenningsstatus, datering for hvert dokument og gjennomgang av forskriftskravene, dato for neste oppdatering og ansvarlige for oppfølging.
- Systematisere dokumentasjonen slik at den er lett å finne frem i og danner en god oversikt over status i enheten.
- Revideres jevnlig. Det anbefales en årlig revisjonssyklus.

Kvalitetssystemets oppbygging tilpasses KBO-enhetens størrelse og behov, og bør ikke være mer omfattende enn at den blir brukt i det daglige arbeidet. Oppbyggingen bør likevel ikke være enklere enn at kvalitetssystemet også kan fungere som et effektivt og pålitelig oppslagsverk for å dokumentere (for enhetens ledelse og tilsynet) at tiltak er etablert og fulgt.

§1-3 Risiko- og sårbarhetsanalyse

Alle enheter i KBO skal ha oppdaterte risiko- og sårbarhetsanalyser for å identifisere virksomhetens risikopotensiale og de tiltak som effektivt oppfyller kravene i denne forskriften.

Veiledning

Med bakgrunn i beredskapsforskriftens formål, vil risiko- og sårbarhetsanalyser (ROS-analyser) i denne sammenhengen handle om å forebygge og håndtere hendelser av betydning for forsyningssikkerheten. ROS-analyser er verktøyet for å kartlegge forhold som kan true enhetens etterlevelse av denne forskriften.

Gjennomføring av ROS-analyser vil gi enheten en oversikt over risiko- og sårbarhetsforhold som kan redusere eller true enhetens leveringsevne. Formålet med kravet til ROS-analyser innbefatter at det enkelte selskap skal identifisere risiko og sårbarhet ved ekstraordinære hendelser knyttet til teknisk svikt, naturgitt skade, samt tilsiktet og utilsiktet skadeverk, både innenfor og utenfor enhetens egen kontroll. Videre skal analysen inkludere beredskapstiltak nevnt i denne forskriften.

1.3.1 Oppdatert

Arbeidet med ROS-analyser skal være en integrert del av enhetens oppgaver og oppdateres ved alle endringer (systemmessige og organisatoriske endringer, eksternt og internt) som kan påvirke enhetens evne til å fungere i henhold til krav hjemlet i denne forskrift. Ved innføring av nye systemer, skal det gjennomføres ROS-analyser for disse.

Alle analyser bør som minimum være påført datoen den ble ferdigstilt, hvem (funksjon) som hadde ansvaret for gjennomføringen av analysen, hvem som deltok i utarbeidelsen og hvem som godkjente analysen.

Alle ROS-analyser bør som minimum gjennomgås årlig, og det bør være en prosess for at risikovurderingen blir godkjent på ledelsesnivå. Det er viktig å merke seg at forskriften stiller krav om ROS-analyser på flere områder. En overordnet ROS-analyse vil derfor ikke dekke samtlige analysekrav alene.

1.3.2 Identifisere enhetens risikopotensiale - analysenivåer

For å identifisere enhetens risikopotensiale og danne seg et godt bilde over hvilke risikoer og sårbarheter enheten må ta hensyn til, bør ROS-analyser gjennomføres på ulike nivåer.

Analysenivåene kan deles i 3:

- Nivå 1-analysene ligger på et overordnet nivå og danner en fullstendig oversikt over anlegg og kritiske prosesser enheten har ansvar for. Analysen vurderer aktuelle trusler og gjør betraktninger rundt uønskede hendelser som kan sette systemet helt eller delvis ut av drift. Videre bør hvert anlegg og hver kritiske prosess rangeres ut fra viktighet for å opprettholde produksjon og forsyningssikkerhet. En grovanalyse vil oftest være dekkende. Nivå 1-analysene danner grunnlaget for å prioritere i hvilke deler av systemet man starter med nivå 2-analyser.
- Nivå 2-analysene gjennomføres mer detaljert og for avgrensede deler av virkesomheten, for eksempel enkeltanlegg og -aktiviteter. Slike analyser vil i enkelte tilfeller avdekke behov for mer detaljerte ROS-analyser av spesifikke delsystem, komponenter eller aktiviteter.
- Nivå 3-analysene gjennomføres for å gjøre mer detaljerte analyser på komponentnivå. Her kan det for eksempel brukes metoder som feiltre-, hendelsestreanalyse eller andre spesifikke analyseteknikker.

Det er viktig å huske på at analysene skal innbefatte de tiltak som effektivt oppfyller kravene i denne forskriften. For ROS-analyse av klassifiserte anlegg, se § 5-4 Analyse.

1.3.3 Tiltak som effektivt oppfyller kravene i denne forskriften

Beredskapsforskriften stiller blant annet konkrete krav til:

- Tilgang på nok kompetent personell og evne til drift (§§ 3-1, 3-2 og 3-4)
- Evne til gjenoppretting av funksjon (§ 3-5)
- Transportberedskap (§ 3-6)
- Informasjonsberedskap (§3-7)
- Sambandsberedskap (§3-8)
- Adgangskontroll og besøksrestriksjoner (§§ 4-5 og 4-6)
- Sikring av anlegg (§§ 5-1, 5-2, 5-4, 5-5, 5-6 og 5-7)
- Informasjonssikkerhet (§§ 6-1, 6-2, 6-3, 6-5 og 6-6)
- Driftskontrollsystemer (§ 6-4)

Tiltak som må gjennomføres for å etterleve disse kravene avdekkes gjennom kontinuerlig arbeide med ROS-analyser.

1.3.4 Utdypende merknader

1.3.4.1 Gjennomføring, forankring og oppfølging av ROS-analyser

Det er viktig at et representativt utvalg for enheten er delaktig i utarbeidelsen av analysene for å sikre god kvalitet. Arbeidet med analysene forankres i enhetens ledelse og inngår i enhetens virksomhetsstyring, se § 1-1 veiledning. Funnene i ROS-analysene følges gjennom forslag til tiltak for å redusere muligheten for, eller effekt av, uønskede hendelser (tiltaksplan) som ledelsen tar stilling til. Det er ikke mulig å prioritere bort tiltak som må på plass for å tilfredsstille forskriftskravene.

1.3.4.2 Sannsynlighet

§ 1-1 gir pålegg om forebygging av ekstraordinære situasjoner som kan hindre forsyningssikkerheten. At enheten vurderer sannsynligheten for en gitt uønsket hendelse til å være lav, vil likevel ikke si at hendelsen kan utelates fra analysen og beredskapsarbeidet. Ved gjennomføringen av ROS-analyser er det derfor nødvendig at enheten er bevisst på å identifisere sårbarheter. Videre må enheten gjennomføre eventuelle forebyggende og skadereduserende tiltak, selv om sannsynligheten for hendelsen oppfattes som lav.

1.3.4.3 Samarbeid og samordning

Det er viktig at analysene bygger på informasjon fra interne og eksterne kilder med høy kvalitet. I den grad enheten er avhengig av eksterne beredskapstjenester, må dette innarbeides i ROS-analysene.

Det er viktig å være bevisst på at andre samarbeidende virksomheter og myndigheter kan etterspørre resultater fra enhetens ROS-analyse som grunnlag for egne analyser. Her er det nødvendig å tilpasse slike data for brukerens formål, samtidig som sensitiv informasjon skjermes.

1.3.4.4 Dokumentasjon

Kildene for ROS-analysene bør være dokumentert og sporbare.

Analysene bør i utgangspunktet være kjent og tilgjengelig for alle i enheten som måtte ha behov for disse i sitt arbeid med sikkerhet og beredskap.

Sensitive opplysninger må skjermes i henhold til kapittel 6 Informasjonssikkerhet for oppbevaring og håndtering av sensitiv informasjon.

1.3.5 Henvisninger

NVE har utarbeidet en egen temaveiledning og eksempelsamling i ROS-analyser for kraftforsyningen. Veiledningen er tilgjengelig på www.nve.no.

Det finnes en rekke andre standarder, veiledninger og verktøy tilgjengelig. Enheten står fritt til å velge verktøy/metode, men plikter å sikre seg at gjennomføring av ROS-analyser er i tråd med pliktene gitt i denne forskriften.

§1-4 Beredskapsplan

Alle enheter i KBO skal ha en oppdatert og funksjonell beredskapsplan. Beredskapsplanen skal blant annet omfatte forberedelser og tiltak det kan bli nødvendig å iverksette ved ulykker, skader, rasjonering og andre ekstraordinære situasjoner som kan påvirke kraftforsyningens drift og sikkerhet. Beredskapsplanen skal samordnes med blant annet berørte myndigheter og andre relevante aktører.

Veiledning

En beredskapsplan skal blant annet:

- Sikre at enheten etablerer et effektivt ledelses- og innsatsapparat i krisesituasjoner (bl.a. gjennom tydeliggjøring av roller og ansvar)
- Sikre oversikt over tilgjengelige ressurser
- Sikre at enheten utnytter ressurser raskt og effektivt i krisesituasjoner

En beredskapsplan er en samlet fremstilling av forberedelser som er gjort, samt tiltak og fullmakter som kan være nødvendig å iverksette i ekstraordinære situasjoner. Planen bør som minimum inneholde følgende elementer:

- Startfase (hvordan komme i gang, hvem kan iverksette planen/når)
- Oversikt over egen organisasjon og ledelse (med beskrevne funksjoner)
- Varslingsliste (nødvendig kontaktinformasjon)
- Innsatsplaner for forskjellige hendelser
- Ressursoversikt (personell, materiell osv.) med kontaktinformasjon (internt og eksternt)
- Informasjonsberedskap (§ 3-7)
- Evt. delplan for sikring av klassifiserte anlegg
- Fordeling/distribusjon av planene (hvem/hvor)
- Dato for godkjenning/oppdatering med videre

I tillegg bør enheten inkludere følgende elementer:

- Innsatsplaner for ulike hendelser (bl.a. ref. ROS.analysene)
- Delplaner i henhold til plikter gitt i denne forskriften
- Opptrappingsplan knyttet til konkrete hendelser, spesielt med tanke på kravene fastsatt i §§ 4-6 Besøksrestriksjoner, 5-5 Sikringsnivå og 6-4 Særlige krav til driftskontrollsystemer.

Beredskapsplanen bør også inneholde alle utskrifter av tegninger, koblingsskjemaer, oversiktsbilder, med mer som enheten oppfatter som nødvendige i forhold til å håndtere en uønsket situasjon. Dette kan gjerne være i et vedlegg.

For virksomheter som har anlegg på flere ulike geografiske steder, med så stor avstand at de ikke kan vurderes under ett, kan det i tillegg til en sentral beredskapsplan være nødvendig med delplaner for hvert enkelt anlegg.

1.4.1 ROS-analysene

Enhetens ROS-analyser og bakenforliggende krav i denne forskriften forventes å danne grunnlaget for hvordan enheten legger opp arbeidet med beredskapsplanleggingen.

1.4.2 Oppdatert

Arbeidet med beredskapsplan må være en kontinuerlig prosess som involverer alle relevante deler av enheten. Planen forankres hos beredskapsansvarlig og –leder, i henhold til §§ 1-1 Beredskapskonsept og 2-2 Ansvar og mundighet.

Enheten bør gjennomføre regelmessig og nødvendig oppdatering av beredskapsplanen. En plan oppdateres ved alle vesentlige endringer og minst en gang årlig for å kunne anses som oppdatert etter denne forskriften. Beredskapsplanen bør også gjennomgås etter inntrufne hendelser og gjennomførte øvelser.

Beredskapsplanen skal være påført datoen den ble godkjent, hvem som hadde ansvaret for oppdateringer og hvem som godkjente planen.

1.4.3 Funksjonell

Planen bør være godt kjent og lett tilgjengelig for alle som skal bruke den. Det er viktig at beredskapsplanen finnes både elektronisk og på papir. Enheten bør som minimum oppbevare planen på minst to ulike steder hvor krisehåndteringen i enheten kan driftes fra, deriblant på driftssentralen og i reservelokaler.

De deler av planen som må ivareta konfidensialitet skal kun være tilgjengelig for rettmessig bruker.

De deler av planen som skal samordnes med andre, må enten merkes tydelig med krav om beskyttelse og unntak fra offentlighet, eller enheten må sørge for å fjerne slik informasjon før oversendelse.

Tidligere utarbeidet eller oversendt krigsplanverk er gradert og skal fordeles og oppbevares i henhold til krav i sikkerhetsloven.

1.4.4 Test av planen

Beredskapsplanen bør testes med jevne mellomrom. For krav til øvelser, se § 1-5 Øvelse.

1.4.5 Samordning

Relevante deler av beredskapsplanen skal samordnes med blant annet berørte myndigheter og andre relevante aktører. Eksempler på dette er kommune(r), Fylkesmannen, nødetatene og viktige infrastrukturaktører. Den skal også samordnes med Kraftforsyningens distriktssjef (KDS) og systemansvarlig. Videre må planen også tydeliggjøre hvordan eventuelle underleverandører og tilgrensende nettselskap er ment å bidra til KBO-enhetens beredskap. Samordningen er viktigst når det kommer til varslingslister, prioriteringsslister, rasjonering, ressursoversikter, tilgang på personell og materiell og utstyr.

§1-5 Øvelser

Alle enheter i KBO skal gjennomføre øvelser med slikt innhold, omfang og hyppighet at enhetens kompetanse utvikles og vedlikeholdes for at enheten kan løse de oppgaver den kan bli stilt overfor.

Veiledning

Øvelser skal utvikle enhetens evne til å håndtere alle typer ekstraordinære hendelser den kan bli utsatt for. Enheten skal ha en plan som sier hvordan dette forskriftskravet skal oppfylles. En slik plan for øvelser bør si noe om hva enheten skal øve på, når, og med hvilke ressurser. Øvelsesplanen bør bygge på enhetens ROS-analyser, beredskapsplan samt kravene gitt i denne forskriften (eksempelvis krav til samband, transportberedskap med mer). Eksempler på forhold som bør danne grunnlag for øvelsesplanen, er:

- Svakheter avdekket gjennom ROS-analyser
- Beredskapsplan
- Erfaringer fra reelle hendelser
- Erfaringer fra tidligere øvelser
- Erfaringer fra analyser og utredninger
- Sentrale føringer for hva man skal øve på

Øvelsesplanen bør forankres hos ledelsen. Planen bør ha en definert varighet og oppdateres regelmessig. Det er en fordel at planen minst strekker seg over en fireårsperiode, der enheten gjennomfører øvelser hvert år. Det kan være lurt å planlegge for en fullskalaøvelse på slutten av en øvelsessyklus for å bygge opp kompetanse over tid og la en større øvelse oppsummere det man har lært. Beredskapsplanen bør alltid testes under øvelsene.

1.5.1 Planlegging

1.5.1.1 Etablering av planleggingsgruppe

En planleggingsgruppe bør bestå av personer med organisatorisk oversikt, beredskapskompetanse og kunnskaper om aktuelle anlegg (for eksempel representanter fra selskapets ledelse, beredskapskoordinator, stasjonsleder, med flere). Dersom eksterne ressurser som politi og brannvesen skal delta i øvelsen, bør planleggingsgruppen også ha med representanter fra disse. Det er viktig at de som skal øves ikke er med på planleggingen. Under gjennomføringen av øvelsen bør planleggingsgruppen utgjøre øvingsledelsen, ledet av en utpekt øvingsleder.

1.5.1.2 Valg av øvelsesmodell

Utgangspunktet for valg av modell er blant annet hva man ønsker å øve på og tilgjengelige ressurser. Når planleggingsgruppen skal gå i gang med arbeidet, er det en fordel at øvingsmodellen allerede er bestemt og beskrevet i enhetens øvelsesplan/øvelseskalender. Eksempler på øvingsmodeller:

Varsling og rapportering:

Hensikt: Test av samband og kommunikasjon, samt rapportering

Varsling, mobilisering og etablering:

- Hensikt: Teste hvor lang tid det tar å etablere for eksempel en skadestedsledelse, kriseledelse, m.m.

Praktisk øvelse:

- Hensikt: Teste ulike problemstillinger i praksis knyttet til gjennomføring av beredskapsplan – eksempelvis øvelse med havari av anlegg som følge av brann, eksplosjon, naturhendelser, sabotasje eller andre hendelser.

Strategisk skrivebordsøvelse:

- Hensikt: Belyse og drøfte ulike strategiske og praktiske utfordringer med alle involverte uten å måtte iverksette tiltak i praksis. En tids- og kostnadsbesparende øvelse, hvor det ikke er antall deltakere som er avgjørende for resultatet av øvelsen, snarere hvem som deltar

Fullskala spilløvelse:

- Hensikt: Teste både strategiske og operative problemstillinger i praksis, og involvere alle som vil ha en rolle i en krisesituasjon. En tidkrevende og kostbar øvelse som krever mye ressurser, men som er spesielt godt egnet til å avdekke egen beredskapsstatus

Samordnede øvelser:

- Spilløvelser eller diskusjonsøvelser som planlegges og gjennomføres i samarbeid med andre virksomheter eller sektorer (for eksempel kraft, ekom og vei, eller kraft, politi og brannvesen).

1.5.1.3 Målformulering og øvelsesmomenter

I forkant av øvelsen bør det settes opp klare og tydelige mål for gjennomføringen. Disse kan deles inn i et hovedmål og mer avgrensede delmål.

Alle aktører som deltar i øvelsen bør få anledning til å definere egne fag- eller virksomhetsspesifikke delmål, for å sikre at man øver på de riktige tingene og at alle får et godt øvelsesutbytte.

1.5.1.4 Valg av målgruppe

Valg av målgruppe henger tett sammen med hva man ønsker å øve på og hvilken øvingsmodell som er valgt. I løpet av øvelsesplanens periode skal alle ledd i organisasjonen øves. Antall målgrupper for øvelsen bør vurderes nøye, for å gjøre det enklere å gjennomføre øvelsen. Går man for bredt ut, ender det ofte opp med at det ikke blir nok øvingsmomenter til alle og dermed redusert øvingsutbytte for flere.

1.5.2 Gjennomføring

1.5.2.1 Valg av tid og sted

I forkant av øvelsen bør man bli enige om en dato for øvelsen, og kommunisere denne ut til øvelsesdeltakerne i god tid før øvelsen. Ved enkelte øvelser kan det være ønskelig at tidspunktet er et overraskelsesmoment (for eksempel ved varslings- og mobiliseringsøvelser). I slike tifeller kan det være lurt å kommunisere ut et tidsspenn for når øvelsen vil finne sted, for å sikre at så mange som mulig av øvelsesdeltakerne er til stede.

1.5.2.2 Øvelsessted

I dokumentasjonen som sendes ut til øvelsesdeltakerne, må det fremkomme tydelig hvor de skal møte opp (for eksempel der det fremgår av beredskapsplanen at de skal møte opp). Ved blant annet spilløvelser vil de som skal øves gjerne øve ut i fra sine respektive arbeidsplasser. Ved øvelser som krever at personell fysisk rykker ut, er det nødvendig å være ekstra tydelig når det gjelder stedsangivelse.

Ved diskusjonsøvelser er det vanlig å invitere deltakerne til å møte på et stort møterom med god plass til å organisere deltakerne rundt egne avdelings-/sektors-/funksjonsvise bord.

1.5.2.3 Scenario

Et scenario er det som beskriver hva man skal øve på. Et scenario kan for eksempel være en beskrivelse av ekstremvær et sted i landet, med påfølgende samfunnsmessige konsekvenser.

Det er viktig å velge scenarioer som kan få ekstraordinære konsekvenser for enheten. En uønsket hendelse som kan oppstå under daglig drift og som lar seg håndtere med ordinære ressurser, er ikke å betrakte som ekstraordinær. For nærmere beskrivelse av hva en ekstraordinær situasjon er, se 1.1.2 ekstraordinære hendelser.

Det overordnede scenarioet kan gjerne gjøres kjent for øvelsesdeltakerne. Scenarioet må imidlertid ikke være for detaljert, da det kan bidra til å ødelegge øvelsesutbyttet.

1.5.2.4 Dreiebok

Dreieboken er øvingsledelsens verktøy for å drive spillet framover. I dreieboken konkretiseres scenarioet gjennom en liste med innspill og problemstillinger som skal rettes mot øvelsesdeltakerne. Innspillene skal bidra til å drive øvelsen framover, og må derfor presenteres i en naturlig rekkefølge, og på en måte som bidrar til å skape flyt og engasjement i øvelsen. I motsetning til scenarioet anbefales at dreieboken normalt holdes hemmelig for deltakerne.

1.5.2.5 Innspill/problemstillinger

Det er viktig at alle som skal øves mottar tilstrekkelig med innspill underveis i øvelsen, slik at de sikres et godt øvelsesutbytte. Det er derfor lurt å sørge for at alle hovedaktører har med representanter i planleggingen av øvelsen. Avhengig av type øvelse kan innspillene presenteres i plenum på en skjerm, skriftlig, over telefon, gjennom fiktive radio- og tv-sendinger, ved at spillende journalister eller andre aktører tar kontakt, med mer.

1.5.2.6 Øvingsledelse og støtteapparat

Avhengig av øvingsmodell, vil det være nødvendig å dedikere personer til følgende funksjoner:

- Øvingsledelse
- Spillmedia
- Spillpublikum/markører
- Observatører/kontrollører
- Sikkerhet – mennesker, informasjon
- Oppfølging av virkelig presse
- Oppfølging av besøkende/observatører
- Administrativ støtte, slik som transport, bevertning og IKT

1.5.3 Evaluering og oppfølging av resultater

Etter hver øvelse bør det foretas en evaluering. Hva som vektlegges ved evalueringen, bør samsvare med de mål som er etablert for øvelsen. Evalueringen bør ha fokus på å vurdere innsatsen til funksjoner, ikke enkeltpersoner. I tillegg bør følgende momenter evalueres:

- Etterlevelse av beredskapsforskriften
- Øvelsesopplegget, herunder praktisk gjennomføring
- Øvelsesressurser, herunder personell og økonomi
- Deltakere på øvelsen (ble alle involvert?)

Utfordringer og svakheter som avdekkes under evalueringen må følges opp i det videre beredskapsarbeidet.

1.5.4 Henvisninger

Direktiv for øvelser m.m. ved kraftforsyningsanlegg, ved NVE og DSB.

Konsept for regionale beredskapsøvelser, kraft – ekom – vei, NVE, 2.7.2009

Kap 2 Kraftforsyningens beredskapsorganisasjon (KBO)

KBO er statens virkemiddel for å etablere, opprettholde og øve en overordnet organisatorisk struktur som i en ekstraordinær situasjon gir relevante enheter i kraftforsyningen i hele landet myndighet, ansvar og oppgaver.

Kapittel 9 i energiloven er under endring. Dette kan bety påfølgende behov for å justere beskrivelsen av KBO.

For KBO sine oppgaver og organisering i erklært beredskap eller krig, se også instruks for kraftforsyningens beredskapsorganisasjon (FOR 1993-08-13-4121).

§2-1 Oppgaver og organisering

KBO skal forberede, etablere og opprettholde en struktur som gir alle relevante ledd i kraftforsyningen oppgaver og ansvar for effektivt å kunne håndtere ekstraordinære situasjoner i kraftforsyningen med tilhørende vassdragsanlegg.

KBO skal omfatte alle de enheter som forestår produksjon med tilhørende vassdrags-regulering, overføring og distribusjon av elektrisk kraft og fjernvarme etter energiloven. Norges vassdrags- og energidirektorat kan vedta at virksomheter som leverer varer, utfører tjenester eller andre som kan ha betydning for kraftforsyningens drift og sikkerhet, skal inngå i KBO.

KBO skal organiseres som følger:

a) Kraftforsyningens sentrale ledelse (KSL) skal bestå av beredskapsmyndigheten og systemansvarlig,

b) kraftforsyningens regionssjefer (KRS) skal utpekes fra systemansvarlig,

c) kraftforsyningens distriktssjefer (KDS) skal utpekes fra enhet i KBO, og

d) øvrige enheter i KBO.

Veiledning

Denne paragrafen angir ansvarsfordeling og oppgaver innad i KBO-strukturen. Ved ekstraordinære situasjoner som ikke er av nasjonal betydning, erklært beredskap eller krig, kan KBO benyttes for å løse oppgaver. KBO kan da pålegges oppgaver etter § 2-4 Plikt til å følge beredskapsmyndighetens pålegg, selv om det ikke er aktuelt å underlegge kraftforsyningen KBO etter energiloven kapittel 9.

2.1.1 KBO-enheten

KBO består av alle enheter som driver produksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk energi og fjernvarme av betydning for landets kraftforsyning. For andre virksomheter som leverer varer og tjenester som har betydning for kraftforsyningens drift og sikkerhet, er det imidlertid nødvendig med vedtak fra NVE i henhold til § 2-2 første ledd annet punktum i denne forskrift, for at slike virksomheter skal inngå som KBO-enhet.

Den enkelte KBO-enheten har ansvar for:

- Å prioritere håndteringen av ekstraordinære situasjoner når disse oppstår.
- Å opprettholde normal forsyning, eller gjenopprette normal forsyning så snart som mulig.
- Å innlede nødvendig samarbeid med kommunen(e) i forsyningsområdet.
- Å følge gitt eller planlagt prioritering for energileveranser i knapphetssituasjoner. (Der det er flere kommuner i forsyningsområdet og partene ikke blir enige om prioriteringer, skal saken tas opp med KDS.)

2.1.2 Kraftforsyningens distriktssjefer (KDS)

Kraftforsyningens distriktssjefer oppnevnes av NVE og er normalt konsernsjef eller leder for nettselskapet som driver det regionale nettet innenfor et større område (distrikt). NVE har utpekt 14 KDSer (oversikt finnes til enhver tid på www.nve.no). Innenfor det geografiske ansvarsområdet til en KDS vil det som hovedregel være både nett-, produksjons- og fjernvarmeselskaper.

NVE utarbeider årlige forventningsbrev til KDS. KDS skal blant annet:

- Ha oversikt over de viktigste beredskapsmessige utfordringene i sitt distrikt.
- Tilrettelegge for samarbeid og samordning mellom KBO-enhetene.
- Bidra med råd og veiledning om sikringstiltak og kriseberedskap.
- Følge opp underliggende KBO-enheter ved krisesituasjoner.

2.1.3 Kraftforsyningens regionssjefer (KRS)

KRS-funksjonen er under vurdering.

Se, inntil videre, instruks for KBO.

2.1.4 Systemansvarlig (Statnett SF)

Systemansvarliges ansvar knyttet til beredskap

- Bistå NVE både som beredskapsmyndighet og rasjoneringsmyndighet
- Varsle NVE ved hendelser
- Utøve systemansvaret ved å sørge for momentan balanse mellom forbruk og produksjon
- Samordne inngrep i nettet for å holde driften gående med minst mulige skadevirkninger og gjenopprette normale driftsforhold ved driftsforstyrrelser og feil i sentral- og regionalnettet
- Iverksette endringer i kraftselskapenes produksjonsprogrammer hvis nødvendig

2.1.5 Kraftforsyningens sentrale ledelse (KSL)

KSL er direkte underlagt OED. KSL skal bestå av beredskapsmyndigheten (NVE) og systemansvarlig (Statnett SF), og ledes av beredskapsmyndigheten (NVE).

KSL skal bestå av:

- Leder for beredskapsmyndigheten eller den vedkommende bemyndiger
- Leder for systemansvarlig eller den vedkommende bemyndiger
- Ved behov - stab bestående av personell med kunnskap og kompetanse som trengs for den gitte situasjonen, fra beredskapsmyndighet, systemansvarlig eller andre aktuelle aktører/etater

KSLs ansvar ved ekstraordinære situasjoner

- Holde Olje- og energidepartementet (OED) underrettet om kraftforsyningssituasjonen
- Iverksette nødvendige beredskapstiltak som følge av den ekstraordinære situasjonen
- Sørge for varsling i KBO-strukturen

2.1.6 Beredskapsmyndigheten (NVE) sitt ansvar

OED har delegert oppgaven som beredskapsmyndighet, med den myndighet som følger av energiloven kapittel 9 til NVE, se delegeringsvedtak av 14. august 2009 nr. 1191.

NVE fører tilsyn med KBO-enhetene, gjennomfører regionale og nasjonale øvelser og bidrar til samordnet beredskapsplanlegging.

NVE skal lede kraftforsyningens sentrale ledelse (KSL) og landets kraftforsyning ved erklært beredskap og i krig.

2.1.7 Henvisninger

Forskrift om planlegging og gjennomføring av rekvisisjon av kraft og tvangsmessige leveringsinnskrenkninger ved kraftrasjonering (rasjoneringsforskriften) (FOR 2001-12-17-1421) med tilhørende veiledning

Innhold i planverket for kraftrasjonering - Nytt vedtak, NVE, datert 6.11.2006

Instruks for kraftforsyningens beredskapsorganisasjon (FOR-1993-08-13-4121), inklusive oppgaver fastsatt av NVE.

§2-2 Ansvar og myndighet

Leder for enhet i KBO skal ha beredskapsansvaret. Enheten skal utpeke en beredskapsleder. Beredskapslederen skal sørge for nødvendig planlegging og utøvelse av beredskapsarbeidet, herunder blant annet etablere og vedlikeholde kontakter med myndigheter og relevante enheter i KBO.

Alle enheter i KBO skal ha en beredskapskoordinator. Beredskapskoordinatoren er enhetens administrative kontaktledd mot Norges vassdrags- og energidirektorat.

Veiledning

Alle enheter i KBO skal til enhver tid ha en utpekt beredskapsleder og beredskapskoordinator, og dette skal være innrapportert til NVE. NVE anbefaler videre at alle funksjoner i enhetens beredskapsorganisasjon har stedfortredere i tilfelle fravær eller behov for avlastning.

2.2.1 Daglig leders ansvar

- Å utpeke en egnet beredskapsleder, dersom leder ikke selv innehar denne oppgaven. Delegering fratar ikke leder for KBO-enheten beredskapsansvaret
- Å påse at kravene i beredskapsforskriften blir fulgt
- Å stille til disposisjon nødvendige ressurser til beredskapsarbeid
- Å påse at enheten har en beredskapskoordinator

2.2.2 Beredskapsleders ansvar

- Å påse at beredskapsforskriften er kjent og forstått i enheten.
- Å påse at enheten følger beredskapsforskriftens krav
- Å etablere og vedlikeholde nødvendig kontakt med myndigheter og relevante KBO-enheter
- Å sikre relevant intern og ekstern informasjonsformidling
- Kriseledelse

2.2.3 Beredskapskoordinators ansvar

- Å være KBO-enhetens administrative kontaktledd mot NVE
- Å motta og videreformidle vedtak, rundskriv og annen informasjon fra NVE til rette vedkommende internt i enheten
- Å påse at NVE til enhver tid har korrekt kontaktinformasjon om KBO-enheten og sentrale KBO-funksjoner i enheten
- Å gi råd internt i organisasjonen i forbindelse med beredskapsarbeidet

§2-3 Plikt til å følge beredskapsmyndighetens pålegg

Alle enheter i KBO plikter å rette seg etter de pålegg som gis av beredskaps-myndigheten.

Veiledning

OED har delegert oppgaven som beredskapsmyndighet, med den myndighet som følger av energiloven kapittel 9 til NVE, se delegeringsvedtak av 14. august 2009-1191.

Kap 3 Ressurser

Bestemmelsene i kapittel 3 skal sikre at hver enhet i KBO har nødvendige ressurser tilgjengelig i ekstraordinære situasjoner. Behovet for raskt tilgjengelige ressurser i slike situasjoner kan være stort. Bestemmelsene krever at enhetene har tilgang til tilstrekkelig antall personell til å kunne drifte kraftforsyningen i ekstraordinære situasjoner og gjenopprette forsyningen ved behov. I tillegg må dette personellet ha den rette kompetansen til å utføre oppgavene sikkert og effektivt. Krav til bemanning og kompetanse til normaldrift følger av forskrift om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften) FOR 2011-03-10-263.

Det skal alltid være sikre arbeidsforhold for mannskap i henhold til arbeidsmiljølovens bestemmelser, forskrift om sikkerhet ved arbeid og drift av elektriske anlegg, og etter forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff, samt utstyr og anlegg som benyttes ved håndteringen.

Enheten må videre ha tilgang til nødvendige komponenter og utstyr til gjenoppretting. Dette inkluderer anleggsdeler, verktøy, transportutstyr, sambandsutstyr, og annet relevant utstyr. Enheten skal også ha en plan for hvordan informasjon om den ekstraordinære situasjonen gis bl.a. til myndigheter, media og berørte brukere.

§3-1 Personell

Alle enheter i KBO skal kunne dekke personellbehovet som kreves for å holde driften gående i ekstraordinære situasjoner. For dette skal det foreligge en plan som omfatter eget personell, innleid personell og eventuelt behov for å få tilført personell fra arbeidsetaten.

Veiledning

For å ta stilling til antall personell og type kompetanse som trengs for å holde driften gående i ekstraordinære situasjoner, anbefales det å lage en prioritert oversikt over hvilke funksjoner som alltid må ivaretas. Behovet for personell kan inkludere blant annet kriseledelse, reparasjon, gjenoppretting av driften og å holde driftssentralfunksjoner i gang.

3.1.1 Personellbehovet i ekstraordinære situasjoner

Det skal foreligge en dokumentert oversikt over personellbehovet til de ulike funksjonene som må dekkes i ekstraordinære situasjoner. Planen bør bygge på oversikten over hvilke funksjoner som alltid må ivaretas, og må minst inneholde:

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

Personellplanen bør oppdateres minst en gang i året.

I den utstrekning enheten er avhengig av personell utenfor egen virksomhet, må enheten utarbeide en tilsvarende personellplan for disse. Enheten må lage avtaler om prioritet, slik at enheten sikres det innleide personellet i ekstraordinære situasjoner, se også § 3-2 Kompetanse.

Beredskapsorganisasjonens ledelsesoppsetning må være så stor at et utholdende vaktsystem kan bli etablert.

Etter hvert som kompetansekravene har økt, blir det mindre aktuelt å få tilført personell fra ”arbeidsetaten” (nå Arbeids- og velferdsforvaltningen, NAV).

I lov om forsynings- og beredskapstiltak (LOV 1956-12-14-07) §§ 30-32, er det gitt adgang til i fred å foreta registrering av sivil arbeidskraft med pålegg om å møte på angitt sted i en beredskapssituasjon. Selskaper som har behov for å få tilført personell utenfra ved beredskap og krig bør oppgi sitt tilleggsbehov til NAV i fylket. Om mulig bør selskapene gi konkrete forslag, fortrinnsvis basert på frivillighet, på personer man ønsker å knytte til seg ved krigsberedskap. Tildelt personell registreres på samme måte som ansatte i selskapet.

I lov om arbeids- og velferdsforvaltningen (NAV-loven) (LOV-2006-06-16-20) § 10 Beredskap i Arbeids- og velferdsetaten, heter det blant annet: ”Direktoratet skal sikre arbeidskraftbehovet til samfunnsviktige virksomheter ved krise i fred eller krig, samt opprettholde systemer for kartlegging av samfunnsmessige bedrifter og deres behov.”

§3-2 Kompetanse

Alle enheter i KBO skal ha personell med den kompetanse som kreves i ulike funksjoner for å kunne gjennomføre oppgaver i forbindelser med ulykker, skader og andre ekstraordinære situasjoner på en sikker og effektiv måte.

Veiledning

Enheten må ha kompetanse for å sikre ivaretakelse av alle krav i beredskapsforskriften, slik at enheten kan håndtere ulykker, skader og andre ekstraordinære situasjoner som hindrer kraftforsyningen.

Enheten bør herunder ta hensyn til at kritisk viktige medarbeidere kan være forhindret fra å stille opp i en ekstraordinær situasjon, eller har sluttet.

KBO-enheten skal selv ha sentral kompetanse for håndtering av ekstraordinære situasjoner. Enheten kan velge om ytterligere tilgang på personell og kompetanse skal sikres gjennom eget personell og innleid personell eller gjennom samarbeidsavtaler. Dette forutsetter at enheten utfører oppgavene sikkert og effektivt, og følger øvrig lovgivning som setter krav til kompetanse og bemanning. Legg merke til at kompetansekravet blant annet omfatter så ulike forhold som:

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

I en beredskapssituasjon må enheten ha sikker tilgang på fagfolk som har erfaring i å betjene anleggene ved lokalstyring.

3.2.1 Kompetansekrav til lederfunksjoner

Daglig leder, beredskapsleder, beredskapskoordinator og IT-sikkerhetsleder vil kunne utgjøre kjernekompetansen for styring av enheten gjennom ekstraordinære situasjoner.

3.2.1.1 Daglig leder

Daglig leder har ansvar for at enheten etterlever beredskapsforskriftens krav, og bør:

- Kjenne til forskriftens krav.
- Sørge for at enheten har kompetanse i hvordan forskriftens krav forstås og håndteres.

3.2.1.2 Beredskapsleder

Beredskapsleder skal planlegge og utøve beredskapsarbeidet, og bør:

- Ha inngående kunnskap til beredskapsforskriftens krav.
- Ha kjennskap til kraftforsyningen.
- Ha god oversikt over enhetens beredskapsstatus og beredskapsorganisasjon.
- Holde seg oppdatert innenfor beredskap og krisehåndtering.

3.2.1.3 Beredskapskoordinator

Beredskapskoordinatoren bør:

- Ha generell oversikt og inngående kunnskap til gjeldende lover og forskrifter innenfor sikkerhet og beredskap i kraftforsyningen, samt til interne krav til beredskaps- og sikkerhetsarbeidet

Beredskapskoordinator trenger likevel ikke ha detaljkunnskaper innenfor hvert enkelt område.

3.2.1.4 IT-sikkerhetsleder

IT-sikkerhetsleder har viktige oppgaver innenfor oppfølging av IKT-sikkerhet, driftskontrollsystem og administrative systemer som inneholder viktig eller sensitiv informasjon, se 6.1.6 IT-sikkerhetsleder. IT-sikkerhetsleder bør derfor ha:

- Gode kunnskaper om enhetens driftskontrollfunksjoner og administrative datasystemer, deres funksjonalitet, og hvordan de skal beskyttes
- Kjennskap til trusselbildet.

3.2.2 Henvisninger

Forskrift om krav til kompetanse mv. hos anleggs- og områdekonsesjonærer (kompetanseforskriften), FOR 2011-03-10-263.

§3-3 Fritaksordninger

Etter søknad fra enhet i KBO kan personell som er viktig for å opprettholde driften av kraftforsyningen i krig, få utsettelse med eller fritak for fremmøte i Forsvaret ved mobilisering. Etter søknad fra enhet i KBO kan dette personellet også få fritak for tjeneste i sivilforsvaret og politireserven.

Personell i KBO som er gitt utsettelse med eller fritak for annen beredskapstjeneste skal registreres ved bruk av sivilt krigstjenestekort. Personell som inngår i KBO skal utstyres med personlig utstyr.

Tjeneste i KBO innebærer tjenesteplikt ved øvelser og mobilisering for den enkelte på lik linje med annen tjeneste i totalforsvarets beredskapsorganer.

Veiledning

3.3.1 Fritak eller utsettelse av fremmøte i Forsvaret ved mobilisering

Personell som er viktig for driften av kraftforsyningen i krig, vil etter melding/søknad kunne bli gitt fritak for eller utsettelse av fremmøte i Forsvaret ved mobilisering. For å kunne være en del av fritaksordningen må enheten ha utarbeidet:

- Beredskapsplan hvor beredskapsorganisasjonen fremgår.
- Plan for hvordan arbeidskraftbehovet ved krigsberedskap skal dekkes.

Enheten må fylle ut Blankett 4071b som kan lastes ned på www.nve.no eller www.mil.no, og sende denne inn til NVE ved Beredskapsseksjonen.

Regler om fritak og utsettelse er gitt i Tjenestereglement for Forsvaret, gruppe 52, undergruppe 523. Siste revisjon er datert 1.august 2001. Ordningen med bruk av sivilt krigstjenestekort, som refereres til i denne bestemmelsen, er utgått.

Personell får innvilget fritak og utsettelse for ett kalenderår (mobiliseringstermin) om gangen. Det er ikke nødvendig å melde inn personer som er godkjent i ordningen året før, på nytt, dersom ikke spesielle forhold tilsier det. Kraftforsyningen er tildelt en kvote som NVE fordeler på grunnlag av innsendte meldinger fra KBO-enhetene. Den tildelte kvoten er kun ment å dekke det viktigste og mest uerstattelige personellet, som eksempelvis driftspersonell.

Personell som kommer inn under ordningen er inndelt i to hovedgrupper:

Gruppe	Generelt gjelder dette for	For kraftforsyningen	Type fritak
1	Spesifiserte samfunnsviktige stillinger/verv i det offentlige som bare kan ivaretas av personer som innehar funksjonen i fred, eller er utpekt ved mobilisering.	Stillinger i KBO-enhetene, noen stillinger i NVE, samt regionssjefer hos systemansvarlig selskap og KDS med stedfortredere.	Fritatt for fremmøte i Forsvaret ved mobilisering og for all tjeneste i fred, såfremt melding om forholdet skjer etter ovennevnte betingelser og regler.
2	Funksjoner i det offentlige/private der det beredskapsmessig er påkrevd at et minimum av nøkkelpersonell, ut over Gruppe 1, kan fortsette i sine funksjoner, eller settes i andre utpekte funksjoner ved mobilisering.	Kraftforsyningens driftspersonell og andre nøkkelpersoner som ikke kan unnværes ved beredskap og krig	Gis utsettelse med fremmøte i Forsvaret ved mobilisering for et nærmere avtalt tidsrom eller inntil videre. Søknad om utsettelse er foreslått tatt ut. Enten fritak eller avslag etter ny modell. Etter utgangen av året de fyller 30, vil de være fritatt for repetisjons- og heimevernsøvelser med mer, i fred.

Vernepliktig personell under Gruppe 2 er, ut fra sin militære status, inndelt i 2 undergrupper, gruppe 2A og 2B:

Gruppe	Dette gjelder	Fritak
2A	Korporaler (tilsvarende) og menige.	Det kan søkes om utsettelse innen rammen av tildelte kvoter. Her er det også forslag til justering, søknad om utsettelse utgår. Forsvarets overkommando kan bestemme at nærmere angitte årsklasser og militære fagkategorier skal være unntatt fra ordningen.
2B	Befal, samt korporaler (tilsvarende) og menige som er mobiliseringsdisponert som befal. Korporaler (tilsvarende) og menige som det er behov for å søke om utsettelse for, men som ikke har fått plass innenfor rammen av kvoter under 2A.	Utsettelse under Gruppe 2B vil bli gitt under forutsetning av at Forsvaret finner å kunne unnvære personellet i sine mobiliseringsoppsetninger.

Enheten kan klage på avslag. Hver høst, når registerutskriftene for påfølgende mobiliseringstermin foreligger, vil enhetene få retningslinjene og fristene for klageadgangen. Ved klage skal enheten benytte Blankett 4072 – ”Klage over avslag på søknad om utsettelse (Gruppe 2B) med fremmøte i Forsvaret ved mobilisering", som kan lastes ned på www.nve.no og www.mil.no.

3.3.2 Fritak for tjeneste i Sivilforsvaret og Politireserven

I henhold til kongelig resolusjon av 24. mai 1985 kan nøkkelpersonell i kraftforsyningen bli fritatt for tjeneste i Sivilforsvaret. Ordningen er ment å gi fritak for det viktigste og vanskeligst erstattelige personellet.

- Hver KBO-enhet sender skriftlig melding til vedkommende sivilforsvarskrets om nøkkelpersonell som ønskes fritatt for tjeneste i Sivilforsvaret.
- Meldingen skal gi opplysninger om navn, fødselsnummer (11 siffer) og stilling i selskapets beredskapsorganisasjon.
- Dersom den fritatte fratrer sin stilling, plikter både vedkommende og KBO-enheten å melde fra til sivilforsvarskretsen om dette.

Nøkkelpersonell i kraftforsyningen kan på liknende måte søkes fritatt for tjeneste i Politireserven. Søknaden skal da sendes til det relevante politidistriktet.

3.3.3 Plikter for fritatt personell

Tjeneste i KBO innebærer tjenesteplikt og møteplikt ved øvelser og mobilisering for den enkelte på lik linje med annen tjeneste i Totalforsvarets beredskapsorganer, se Lov om forsynings- og beredskapstiltak (LOV 1956-12-14 nr 07) § 13. Fritatt personell plikter derfor å delta i øvelser arrangert i KBO-enheten. Dette gjelder øvelser KBO-enheten selv organiserer, øvelser i distriktet arrangert av KDS, og nasjonale øvelser der NVE er arrangør eller deltaker.

3.3.4 Personlig utstyr

Personell i KBO skal ha nødvendig personlig utstyr, både av verne- og førstehjelpsutstyr. Enheten må selv vurdere hvilket utstyr som er nødvendig for sitt personell, men bør beholde eksisterende utstyr som er i tilfredsstillende stand. Enheten bør oppbevare personlig utstyr tilgjengelig og gi personellet opplæring i hvordan utstyret brukes.

§3-4 Drift

Alle enheter i KBO skal i ekstraordinære situasjoner effektivt kunne drive de kraftforsyningsanlegg og den del av kraftsystemet enheten har ansvaret for. Enheten skal planlegge og etablere en organisasjon med kompetanse, utholdenhet og ressurser til å gjennomføre de oppgaver dette krever på en sikker og effektiv måte.

Kraftforsyningsanlegg, utstyr og øvrige ressurser av betydning for drift og sikkerhet skal holdes i forsvarlig stand. Dette utstyret og ressursene skal være tilgjengelig for enheten.

Veiledning

Hovedhensikten med denne bestemmelsen er å sørge for at kraftforsyningen har en høy grad av sikkerhet også i ekstraordinære situasjoner.

3.4.1 Sikker og effektiv drift

For å oppnå sikker og effektiv drift må enheten:

- Ha dokumenterte planer for drift med nødvendige ressurser under ekstraordinære situasjoner
- Ha etablert en organisasjon med forutsetninger for å kunne gjennomføre drift også i ekstraordinære situasjoner.
- Sørge for sikre arbeidsforhold for mannskap i henhold til arbeidsmiljølovens bestemmelser, forskrift om sikkerhet ved arbeid og drift av elektriske anlegg (FOR 2006-04-28-458), forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff, samt utstyr og anlegg som benyttes ved håndteringen (FOR-2009-06-08-602) § 7 Kompetanse, siste ledd.

3.4.2 Om kompetanse og utholdenhet

Organisasjonen må ha tilstrekkelig med kompetent driftspersonell, se §§ 3-1 Personell og 3-2 Kompetanse. Enheten må:

- Sikre at de har så mange personer tilgjengelig at det blir mulig å greie seg gjennom langvarige situasjoner, eksempelvis en rasjoneringssituasjon med sonevis roterende utkobling i flere uker.
- Kunne håndtere ekstraordinært press over lang tid, for eksempel dersom det oppstår flere driftsfeil samtidig.

Enheten bør ta høyde for samtidige hendelser.

Eksempel på samtidige hendelser:

Uvær slår ut flere forsyningslinjer.

Ras som rammer en kraftlinje samtidig med svikt i driftskontrollsystemet.

Teknisk svikt på flere forsyningslinjer til samme område.

Stort rørbrudd og sterk kulde.

Enheten bør også ta høyde for at en, eller flere sammenfallende hendelser, kan ramme flere selskaper innen samme geografiske område. Dette er et hensyn som særlig bør ivaretas i forhold til tilgang på personell.

3.4.3 Forsvarlig stand

Alle anlegg og alt utstyr som er nødvendig for at sikrings- og beredskapstiltak skal fungere i ekstraordinære situasjoner, skal holdes i forsvarlig stand og fungere etter forutsetningene. Enheten bør gjennomføre systematisk vedlikehold, modernisering eller erstatte gammelt utstyr med nytt, slik at dette utstyret og anleggene fungerer etter hensikten når behovet oppstår. Enheten bør legge spesiell vekt på dette når utstyret sjelden er i bruk. Se også § 5-7 Kontroll og vedlikehold.

3.4.4 Tilgjengelighet

Enheten skal oppbevare ovennevnte utstyr og ressurser slik at det er tilgjengelig for rask bruk, og med egnet transportberedskap. Ressurser inkluderer materiell og verktøy, ledelsesressurser, kompetanse og personell. Det er et krav at disse ressursene er tilgjengelige i ekstraordinære situasjoner, også om de leveres av en underleverandør.

3.4.5 Bemanning av driftssentraler

Driftssentraler i klasse 3 skal, av hensyn til beredskapen i ekstraordinære situasjoner til enhver tid være døgnbemannet, fortrinnsvis med *minst* to personer. Driftssentraler i klasse 2 bør også være døgnbemannet

§3-5 Gjenoppretting av funksjon

Alle enheter i KBO skal på kort varsel kunne fremskaffe nødvendig antall egnede og kompetente personer til å gjenopprette nødvendige funksjoner ved de kraftforsyningsanlegg og den del av kraftsystemet enheten har ansvaret for.

Enheten skal ha den nødvendige oversikt over og tilgang til reservedeler, reparasjonsutstyr og øvrige ressurser som trengs for å gjennomføre dette på en sikker og effektiv måte. Reservemateriell og andre nødvendige ressurser for gjenoppretting av funksjon skal holdes i forsvarlig stand og klar til bruk.

Enheten skal kunne dokumentere de kraftforsyningsanlegg og den delen av kraftsystemet den har ansvaret for, herunder blant annet prioriterte kunder, utkoblbar last, koblingsbilder og flaskehalser

Veiledning

Hovedhensikten med denne bestemmelsen er å sørge for at kraftforsyningen 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. Dette betyr både at anleggets funksjonalitet skal gjenopprettes og at ødelagte komponenter repareres eller erstattes. Anleggets funksjonalitet skal gjenopprettes innen rimelig tid, raskt eller straks avhengig av anleggets klasse, i henhold til § 5-5 Sikringsnivå.

For å oppnå sikker og effektiv gjenoppretting må enheten:

- Ha dokumenterte planer for gjenoppretting.
- Ha etablert en organisasjon med forutsetninger for å kunne gjennomføre gjenoppretting også i ekstraordinære situasjoner.
- Sørge for sikre arbeidsforhold for mannskapet; i henhold til bestemmelser i arbeidsmiljøloven, forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg og i forskrift om håndtering av brannfarlig, reaksjonsfarlig og trykksatt stoff, samt utstyr og anlegg som benyttes ved håndteringen - §7. Kompetanse, siste ledd.

3.5.1 Ressurser

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

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

- Mobile varmesentraler.
- Datakomponenter og programvare for kritiske funksjoner.

Det er ikke et krav at enheten selv har alt dette, men enheten må vurdere behovet og sikre seg tilgang. Hvis enheten ikke selv har disse ressursene, må det inngås skriftlige avtaler med leverandører, eller andre everk om gjensidig hjelp. Enheten må sørge for at leverandører av kritiske 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.

Medlemmer av e*Beredskap* har materiell og utstyr i en database som viser hva som er tilgjengelig.

Reserve- og beredskapsmateriell det er gitt tilskudd til, skal være tilgjengelig for andre enheter i KBO.

Der det ikke er mulig med rask omkobling eller reparasjon for å få forsyningen tilbake til prioriterte kunder (liv og helse), bør enheten ha et system for bruk av aggregat.

3.5.2 Oversikt og dokumentasjon

Enheten må ha en oversikt over tilgjengelige hovedressurser. Det er viktig at oversikten holdes oppdatert. Kravet gjelder ikke bare kraftforsyningssystem og anlegg, men også driftskontrollsystemet med samband, relévern, driftsradio og andre nødvendige systemer. Ressursene kan deles inn i følgende grupper:

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

Enheten må gjennomføre systematisk kontroll og vedlikehold av ovennevnte utstyr.

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

3.5.3 Reparasjonsberedskap i driftskontrollsystemer

For driftskontrollsystemets mest vitale og mest utsatte enkeltkomponenter etableres særskilt reparasjonsberedskap, enten i eget selskap eller kontraktfestet hos ekstern leverandør.

3.5.4 Reparasjonsberedskap i sentral- og regionalnettet med tilgrensende kraftstasjoner

For å oppnå god reparasjonsberedskap, er det nødvendig at alle forhold listet opp nedenfor er oppdatert, godt forberedt og innøvd. Ressursene må være tilstrekkelige og tilgjengelige i ekstraordinære situasjoner. Hver enkelt KBO-enhet bør på forhånd gjennomføre en egen vurdering og bestemme akseptabel responstid for startfasen etter en uønsket hendelse og dokumentere dette i beredskapsplanen. Uakseptable responstider og reparasjonstider vil identifiseres gjennom dette arbeidet. KBO-enheten bør treffe risikoreduserende tiltak der det viser seg nødvendig. Det som er angitt i 3.5.4.1 til 3.5.5.5 skal være forberedt.

3.5.4.1 Personressurser, kapasitet over tid

Enheten må sikre seg tilstrekkelig kompetanse, herunder:

- Egne ansatte og ansatte i samme konsern.
- Innleide (beredskapsavtale og opptrappingsplan med entreprenører).
- Samarbeidsavtaler (med andre nettselskaper).
- Responstid.
- Utholdenhet.

3.5.4.2 Kompetanse

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

3.5.4.3 Materiell

Enheten må sikre seg nødvendig materiell, herunder:

- Beredskapslager med kritisk materiell og materiell med lang leveringstid.
- Leverandører med eget lager.
- Nasjonal samarbeidsordning om beredskapsmateriell; e*Beredskap*.
- Regionale og andre samarbeidsavtaler om materiell.
- Beredskapsmaster, reservetransformatorer, effektbryter, kabelskjøter, etc.
- Korrekt lagring av materiell må spesifiseres.
- Oppbevare beredskaps- og reservemateriell slik at ikke samme hendelse ødelegger både dette materiellet og de komponenter materiellet er reserve for.

3.5.4.4 Forberedte tiltak

Enheten må forberede tiltak, herunder:

- Spesielle / samtidige / ekstraordinære hendelser skal vurderes.
- Beredskapsplaner for ekstraordinære hendelser.
- Øvelser.
- Forberedte nødløsninger / provisorier, "verktøykasse" med alternative løsninger. (Forbikobling av brytere og måletransformatorer, omstilling av vern).
- Forberedte løsninger ved arbeid i nettet for å kunne gjenopprette eller koble om når feil oppstår.
- Produksjon med innmating i nettet.
- Plan for å ta imot bistand.

3.5.4.5 Kriseledelse

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

3.5.4.6 Administrativt

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

3.5.4.7 Produksjon

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

3.5.4.8 Forventninger til respons

- Forventet tid til oppdagelse i alle systemer, straks.
- Forventet tid fra feilen har skjedd til provisorisk forsyning kan gjenopprettes, opp til 1-2 døgn.
- Tilgang på alle nødvendige ressurser.

Tidene nedenfor bør være mulig å oppnå for alle feilsituasjoner i sentral- og regionalnettet og alle klasser av anlegg. For alle viktige anlegg og når det er avbrudd i forsyningen til et stort antall sluttbrukere, forventes nedre del av de angitte tider.
Ved redundans i systemet eller når N÷1-kriteriet er oppfylt, gjenopprettes forsyningen øyeblikkelig og automatisk eller ved kobling. Når systemet ikke har redundans (er forsynt radielt), skal enheten legge stor vekt på å ha forberedt provisorisk forsyning. I enkelte feiltilfeller hvor det i utgangspunktet er bygget med redundans, kan likevel funksjonaliteten rammes hvis flere redundante komponenter rammes.

Nedenfor er responstidene skissert for ulike situasjoner, avhengig av driftskontrollsystemets klasse, om N-1-kriteriet er oppfylt, om sluttbrukere rammes, omfang, og delt opp på type anlegg og fasene i omkobling og reparasjon.

Klasse 3 driftskontroll - omkobling er mulig

- Oppdage hendelsen straks i driftssentral / driftskontrollsystem, jf § 5-5 c) Sikringsnivå klasse 3.
- Vurdere situasjonen og foreta omkobling straks for å gjenopprette forsyningen (anslagsvis 1 minutt til 1 time).
- I stasjonsanlegg kan det være nødvendig å sende ut mannskaper straks for å se omfanget / hvilken del av stasjonsanlegget som er "friskt" før innkobling foretas, ½ - 1 time.
- Videre reaksjonsmønster i henhold til beredskapsplan, jf § 1-4 Beredskapsplan, med angitte beredskapstiltak og responstider.
- Kun unntaksvis er kundene uten strøm mer enn 1-2 timer ved slike feil i sentral- og regionalnett. Hvis dette ikke er tilfelle, se feil som medfører avbrudd i forsyningen, under.
- Etter gjennomført startfase kan det ta dager til måneder for å gjenopprette status før feilen – se nedenfor for reparasjon.

Klasse 2 driftskontroll - omkobling er mulig

- Oppdage hendelse raskt i driftssentral/driftskontrollsystem, (anslagsvis 1 til 15 minutter), jf § 5-5 b) Sikringsnivå klasse 2.
- Vurdere hendelsen og iverksette innledende tiltak raskt, (anslagsvis 10 til 15 minutter).
- Videre reaksjonsmønster i henhold til beredskapsplan, jf § 1-4 Beredskapsplan, med angitte beredskapstiltak og responstider.

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

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

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

Avbrudd med stort omfang

- Innledende faser som over.
- Etablere krisestab.
- Sende ut mannskaper for å se omfanget og vurdere tiltak, (anslagsvis 1/2 til 2 timer avhengig av vær).
- Innkalle beredskapsressurser (materiell og mannskaper).
- Iverksette eventuelle midlertidige løsninger (kabler på bakken, provisoriske koblingsanlegg).

Reparasjonsfasen

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

Produksjonsanlegg i klasse 2 og 3

- Oppdage hendelsen straks i driftskontrollsystemet.
- Vurdere situasjonen, iverksette innledende tiltak raskt.
- 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 omfanget og hvilke del av anlegget som er "friskt" for innkobling, ½ til 3 timer.
- Gjøre beslutninger om videre tiltak, neste arbeidsdag.
- Innkalle relevante beredskapsressurser (materiell og mannskaper).
- Igangsette reparasjonsarbeider.
- Deretter kan det ta dager til måneder for å gjenopprette status før feilen.

3.5.5 Reparasjonsberedskap for distribusjonsnett og fjernvarme

Forventninger 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 ikke omkoblingsmuligheter. Det er derfor av like stor betydning å:

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

Forventninger til responstid for sentral- og regionalnett med kraftstasjoner gitt over, bør legges til grunn. I tillegg må det i distribusjonsnettet legges stor vekt på aggregatdrift inntil feil er reparert, for at samfunnsviktige funksjoner kan opprettholdes. NVE vil imidlertid samtidig presisere at alle sluttbrukere som er kritisk avhengige av kontinuerlig strømforsyning, selv har ansvar for å sikre egen nødstrømforsyning.

3.5.6 Henvisninger

- For krav til kompetanse, se § 3-2 Kompetanse.
- For dimensjonering av gjenopprettingsevnen til anlegg, se § 5-5 Sikringsnivå.
- For krav til tilskuddsmateriell, se § 7-2 Tilskudd til sikringstiltak og anskaffelse av reservemateriell.
- www.eberedskap.no

§3-6 Transport

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

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

Veiledning

Enheten skal ha en plan for transportberedskap. Planen bør inneholde oversikt over:

- Kjøretøyer og transportutstyr som selskapet 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.
- Eventuelt andre forhold enheten finner relevant.

Det er svært viktig at transportberedskapsplanen er gjennomførbar. Det vil blant annet si at planen må forberede beredskap for alternative transportruter ved transport av eksempelvis transformatorer med andre ytre mål enn det som har vært vanlig på norske veier.

Der enheten er avhengig av eksterne ressurser, anbefales det å kontraktfeste dette.

3.6.1 Transport av komponenter med transportvekt anslagsvis over 70 tonn

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

- Type last.
- Vekt og største ytre dimensjoner.
- Opp- og avlastingssted.
- Beskrive opplastingsplass og transportrute med angivelse av spesielle forhold.
- Hvilket utstyr som skal brukes.
- Kjøretillatelser.

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

Statnett SF skal opprettholde en tungtransportberedskap i KBO som på kort varsel skal kunne dekke kraftforsyningens behov for transport av tunge enheter i fred, ved beredskap, og i krig. Retningslinjer for tungtransportberedskap i kraftforsyningen er fastlagt av Olje- og energidepartementet, 28.11.1995, og er gjengitt i vedlegg til denne veiledningen

3.6.2 Tilgang til drivstoff

I en krisesituasjon vil bensinstasjonene kunne gå tomme for drivstoff før rasjonering settes i verk. Det er opp til hver enkelt enhet å skaffe seg nødvendig tilgang til drivstoff. Enheten bør derfor vurdere å ha eget drivstoffanlegg, eller inngå avtale om prioritet hos leverandør av drivstoff. Rasjonering av drivstoff kan settes inn ved erklært beredskap og forutsettes satt inn i krig, etter forskrift for oljerasjonering ved beredskap og krig (FOR 1983-12-15 nr 2142). Under knapphetssituasjoner i fredstid gjelder forskrift om oljerasjonering ved oljeforsyningskriser i fredstid (FOR 1983-08-01 nr 2141), § 6.

3.6.3 Forberedt rekvirering av sivile kjøretøyer

Forsvaret, Sivilforsvaret og enkelte andre etater innen totalforsvaret kan ved krigsberedskap rekvirere sivile kjøretøyer. Kjøretøyer som tilhører KBO-enheter, og private kjøretøyer til nøkkelpersonell som av tjenestlige grunner har behov for egen transport, er fritatt for forberedt rekvirering. Fritaket er hjemlet i Lov om militære rekvisisjoner (LOV 1951-06-29-19) §§ 1 og 5. Forberedelse til rekvirering utføres etter Håndbok for forberedt rekvirering av sivile kjøretøyer (TH 100-12), Forsvarets Logistikkorganisasjon, 1984, ved kode 911 og 934.

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

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

Se nærmere om dette hos Statens Vegvesen, omregistrering av kjøretøyer, kodehefte autosys, kap 03, kjøretøyer som er fritatt fra militære rekvisisjoner, pkt. 14.

3.6.4 Sivil transportberedskap

Den regionale myndigheten for sivil transportberedskap er Fylkeskommunen, se forskrift for sivil transportberedskap (FOR 2005-06-14-548). For at kraftforsyningens behov for kjøretøyer, drivstoff og reparasjonsberedskap i en ekstraordinær situasjon skal inngå i

Fylkeskommunens plan, kan KBO-enhetens transportberedskapsplan samordnes med Fylkeskommunen.

§3-7 Informasjon

Alle enheter i KBO skal ha en informasjonsplan og en effektiv informasjonsberedskap i ekstraordinære situasjoner. Dette skal blant annet omfatte informasjon internt i enheten, til berørte myndigheter, publikum og media, samt råd og anvisninger til kundene.

Veiledning

Hensikten med bestemmelsen er å sikre at enhetene i ekstraordinære situasjoner raskt kan iverksette målrettede informasjonstiltak.

3.7.1 Informasjonsplan

Enheten skal ha en plan for informasjonsberedskap. Planen bør inneholde:

- Mål for informasjonsberedskap.
- Koblinger til andre beredskapsplaner.
- Ansvarsfordeling.
- Varslingsliste som inkluderer enhetens informasjonsansvarlig, kriseteam, pressetalspersoner, ansatte som kan bemanne mottakstelefon og sentralbordstjeneste.
- Oversikt over andre tilgjengelige ressurser.
- Oversikt over målgrupper for informasjonen med kontaktinformasjon (media, myndigheter, kritiske forbrukere).
- Rutiner for håndtering av henvendelser fra ovennevnte målgrupper.
- Oversikt over muligheter for distribusjon av informasjon, også alternativer til elektronisk formidling.
- Sjekklister og maler.

Planen bør være forankret i ledelsen.

Enheten bør vurdere hvilke konsekvenser et strømbrudd har for de vanlige informasjons- og kommunikasjonskanalene, og ha beredskap for å møte disse.

3.7.2 Effektiv informasjonsberedskap

Informasjonsansvarlig bør være en del av kriseledelsen. Vedkommende må alltid være fullt oppdatert. Informasjonsstaben bør være i nærheten av kriseledelsen for nødvendig kommunikasjon og avklaring. Den bør være atskilt fra driftssentralen.

Informasjonsstaben bør ha:

- God kapasitet på sentralbordet for henvendelser fra berørte kunder/pårørende/presse. Flere enheter har skaffet seg eget telefonnummer for rapportering av feil.
- Disponibelt lokale med nødvendig utstyr, eksempelvis PCer, telefoner, projektorer, flere internett- og telefonlinjer, med mer.

En beredskapssituasjon i kraftforsyningen vil alltid kreve god koordinering mellom en rekke myndigheter og virksomheter på ulike nivåer. Jo mer omfattende en krisesituasjon er, desto vanskeligere blir det å ha oversikt over roller og ansvar. Det er derfor viktig at enheten blir enig med alle involverte parter om hvem som gir informasjon om hva så tidlig som mulig.

3.7.3 Håndtering av medier

For å håndtere mediene er det viktig å:

- Ha en offensiv holdning og gå aktivt ut med informasjon så tidlig som mulig.
- Være oppmerksom på at den første informasjonen som gis ut i en krise, har stor virkning. Dette stiller krav til at informasjonen er gjennomtenkt.
- Gi oppdatert og riktig informasjon til rett tid og til de rette mottakerne. Skape tillit ved å gi tilstrekkelig innsyn i det som gjøres for å redusere skadevirkninger.
- Være ærlig, påpeke alvoret, ikke bagatellisere. Være ærlig om mulige konsekvenser av hendelsen (for eksempel at det vil ta tid å rette opp feilen, slik at berørte får anledning til å iverksette nødvendige forebyggende tiltak).
- Vise vilje og evne til å ta ansvar.
- Huske at mediene arbeider hele døgnet. Informasjonspersonell bør gå i skift.

Massemediene er ofte de viktigste kanalene til publikum. Erfaring viser at mediene spiller ulike roller under en krise:

- De ”berørte mediene” er opptatt av å hjelpe sine lesere/lyttere. Til de berørte mediene hører nærradio, lokalradio, lokalpresse og til dels regionavisene.
- De nasjonale mediene er ofte mer aktører enn kanaler og fokuserer gjerne på konfliktstoff og det dramatiske. De kan fokusere på å skape motsetninger, fremheve det sensasjonelle, personifisere og utløse følelser hos leseren.

Det lønner seg å spille særlig aktivt på de lokale mediene hvis hensikten er å få gitt nyttig og praktisk informasjon ut til publikum.

3.7.4 Henvisninger

Informasjonsberedskap og strategisk krisekommunikasjon, Direktoratet for samfunnssikkerhet og beredskap (DSB), 2007

Veiledningen til rasjoneringsforskriften på www.nve.no

§3-8 Samband

Alle enheter i KBO 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.

Veiledning

3.8.1 Ekstraordinære situasjoner

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

Enheten skal alltid ha mulighet til å kommunisere med personell som er viktig for å opprettholde kraftforsyningen, også under ekstraordinære situasjoner. Samme krav gjelder for samband mot utstyr eller komponenter for styring av nettet. Ved svikt bør det finnes alternativer som raskt kan etableres. Det er derfor viktig at:

- Driftskontrollsystemene med tilhørende samband fungerer også under ekstraordinære situasjoner.
- Samband opprettholdes selv ved omfattende og langvarige utfall av sambandstjenester som benyttes under normale forhold. I en slik situasjon kan det være behov for å etablere alternativt samband på tvers av sektorer og aktører.
- Anleggene kan betjenes ved lokal styring.
- Alle vern fungerer, se § 6-6 Relésamband – vern av kraftsystem.
- Samband som trengs for å holde komponenter og utstyr i kraftforsyningen i drift virker.

Det er videre viktig at enheten i enhver situasjon har talesamband til alle den trenger å snakke med, for eksempel:

- nødvendig personell som må tilkalles.
- montører og annet personell ute i felten
- personell i stasjoner.
- personell ved andre kontorer i samme KBO-enhet (selskap).
- andre KBO-enheter man har behov for å kommunisere med.
- viktige eksterne leverandører, for eksempel entreprenørselskap og leverandører av driftskontrollsystem.
- Myndighetene.
- Enheten har nødvendig reparasjonsmateriell for sitt sambandssystem.
- Det er tilstrekkelig nødstrøm til sambandssystemene. For konkrete krav til nødstrøm, se § 5-5 Sikringsnivå.
- Enheten er oppmerksom på at mobilnettet kobles ut ved roterende utkobling eller overlast. Det samme gjelder IP-basert telefonnett.

3.8.2 Dokumentasjon, beredskapsforhold og daglig drift

Enheten bør bruke sitt samband i daglig drift for å sikre at personellet som skal bruke sambandet har tilfredsstillende kompetanse til å håndtere det raskt og sikkert. Enheten må minst øve på bruken av samband jevnlig. Sambandet bør brukes ofte nok til at personell klarer å håndtere ekstraordinære situasjoner uten hjelp fra andre kommunikasjonskanaler.

Som hovedregel har overordnet enhet i KBO ansvaret for sambandsforbindelse til underordnet enhet i KBO. KBO-enhetene skal medvirke og ta initiativet dersom sambandsforbindelse ikke er etablert. Kravet til effektive og pålitelige samband gjelder for ledelse, drift og sikkerhet, herunder tale- og datasamband og samband for relévern. Bestemmelsene gjelder i alle situasjoner fra ordinær drift til totalt sammenbrudd i nettet. Minimumskrav til dokumentasjon er:

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

For å være i stand til rask og effektiv håndtering av ekstraordinære situasjoner er det viktig at enheten implementerer sambandsberedskap i beredskapsplanen. I planen må det minst inngå:

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

I tillegg bør planen inneholde rutiner for rotering av personell dersom situasjonen blir langvarig.

3.8.3 Særskilte krav til samband i andre paragrafer

- Krav til sikring av sambandsanleggene mot uønskede hendelser finnes i § 5-5 Sikringsnivå.
- Krav til driftskontrollfunksjoner og driftssamband er presisert i kapittel 6. Informasjonssikkerhet.

3.8.4 Eksterne leverandører av sambandstjenester – avtaler

Ved kjøp av teletjenester til kritiske samband bør vesentlige forhold vedrørende leveransesikkerheten for tjenesten kontraktfestes. Noen forhold som bør avklares er:

- Nødstrøm og reserveforsyning til relevante sentraler og kommunikasjonsnett.
- Redundans, tilgjengelighet (kapasitet, oppetider).
- Prioritet som kan gis ved trafikksperre og feilretting.
- Evne til håndtering av større feil i kritiske situasjoner.
- Andre relevante forhold partene mener bør være i kontrakten.

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

Post- og teletilsynet (PT) har utarbeidet en mal for avtale om tjenestekvalitet: Service leveringsavtale (SLA). Malen er beregnet for bedriftskunder og kan lastes ned fra www.npt.no. Den kan også være nyttig som sjekkliste ved mindre omfattende avtaler.

Kap 4 Sikkerhet

Bestemmelsene i dette kapittelet skal motvirke uønskede hendelser (sikkerhetstruende virksomhet), både tilsiktede og utilsiktede, for å sikre kraftforsyningens ledelse, drift og anlegg. Dette omfatter uaktsomhet, uønsket informasjonsspredning eller – innsamling, urettmessig adgang og spionasje, sabotasje og terrorhandlinger, skadeverk og annen kriminalitet, eller forberedelser til slikt. Nærmere bestemmelser om sikringstiltak er gitt i kapittel 5 Sikringstiltak, og kapittel 6 Informasjonssikkerhet.

§4-1 Ansvar og organisering

Leder for enhet i KBO har sikkerhetsansvaret og skal herunder sørge for å etablere og følge opp sikkerhetsorganisering, rutiner og instrukser.

Veiledning

4.1.1 Daglig leders ansvar

- Sørge for å etablere og følge opp organiseringen av sikkerhets- og beredskapsarbeidet.
- Sørge for at enheten gjennomfører fortløpende totalvurdering av egen sikkerhet og beredskap, samt foretar nødvendige forberedelser og tiltak.
- Se også § 2-3 Ansvar og myndighet

§4-2 Personkontroll

Person som vil kunne få tilgang til informasjon som er sikkerhetsgradert etter lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven), skal være sikkerhetsklarert og ved behov autorisert. Autorisasjon for BEGRENSET kan skje uten forutgående sikkerhetsklarering.

Sikkerhetsklarering og autorisasjon skal gjennomføres etter bestemmelser gitt i og i medhold av sikkerhetsloven.

Veiledning

Hensikten med paragrafen er å sikre at personer som får tilgang til sikkerhetsgradert informasjon er skikket til å motta slik informasjon, og at de kun mottar sikkerhetsgradert informasjon etter tjenstlig behov.

Personkontroll - Innhenting av relevante opplysninger til vurdering av sikkerhetsgradering, etter sikkerhetsloven § 3, første ledd, punkt 15.

Sikkerhetsgradert informasjon - Informasjon som er merket med sikkerhetsgrad i henhold til reglene i sikkerhetsloven § 11, etter sikkerhetsloven § 3, første ledd, punkt 9.

Sikkerhetsklarering - Avgjørelse, foretatt av klareringsmyndighet (NVE) og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad, etter sikkerhetsloven § 3, første ledd, punkt 16.

Autorisasjon - Avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter sikkerhetsklarering, bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov, samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad, etter sikkerhetsloven § 3, første ledd, punkt 17.

4.2.1 Sikkerhetsklarering

En person skal sikkerhetsklareres når vedkommende kan få tilgang til informasjon som er sikkerhetsgradert KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG, gjennom stilling eller oppdrag. Tilgang til informasjon som er sikkerhetsgradert BEGRENSET krever ikke sikkerhetsklarering, men vedkommende skal være autorisert.

4.2.1.1 Fremgangsmåte for sikkerhetsklarering:

- KBO-enheten må skaffe, og den ansatte må fylle ut, Statens personopplysningsblankett (X-0136/1). Opplysningene som gis på blanketten skal være fullstendige og oppriktige. Utelatelse av opplysninger som er av betydning for vurdering av sikkerhetsmessig skikkethet, vil veie tungt i avgjørelsen om klarering.
- Blanketten undertegnes og legges i egen konvolutt merket PERSONKONTROLL.
- Enheten må lukke konvolutten og sende den sammen med undertegnet taushetserklæring (X-0138), og et følgebrev fra KBO-enheten som begrunner behovet og nødvendig nivå for sikkerhetsklarering. Konvolutten sendes til NVE, Beredskapsseksjonen, Postboks 5091 Majorstua, 0301 OSLO.
- NVE avgjør om personen kan sikkerhetsklareres.
- NVE sender kopi av eventuelt klareringsbevis til beredskapskoordinator. Beviset skal oppbevares som et verdidokument.
- Ved avslag sender NVE brev direkte til personen.

Sikkerhetsklareringen er gyldig i 5 år fra utstedelsesdato. Dersom det kommer nye opplysninger av betydning for personens sikkerhetsmessige skikkethet, kan klareringen suspenderes eller tilbaketrekkes.

Personer som innehar gyldig sikkerhetsklarering plikter å opplyse NVE om forhold som kan påvirke sikkerhetsklareringen. Dette kan være økonomiske, strafferettslige eller medisinske forhold, eller endring i sivilstatus. Enheten må sørge for aktiv oppfølging av dette.

4.2.2 Autorisasjon

Før enheten gir den sikkerhetsklarerte personen tilgang til sikkerhetsgradert informasjon, skal personen autoriseres. Den som er eier av informasjonen og skal gi informasjonen til enheten, må sørge for å autorisere aktuelle mottakere. For de fleste KBO-enheter vil dette gjelde informasjon om forsvarsanlegg, og Forsvaret skal da forestå autorisering. Se forskrift om personellsikkerhet, § 5. Autorisasjonen gjelder bare for tjenstlig behov. Dersom personen bytter stilling eller slutter, skal autorisasjonen tilbakekalles.

4.2.3 Personer med utenlandsk statsborgerskap

Utenlandske statsborgere sikkerhetsklareres eller autoriseres ikke etter ovennevnte retningslinjer. En utenlandsk statsborger kan, etter Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) (LOV 1998-03-20-10) § 22 Sikkerhetsklarering av utenlandske statsborgere, gis sikkerhetsklarering etter en vurdering av hjemlandets sikkerhetsmessige betydning, samt vedkommendes tilknytning til hjemlandet og Norge. I slike tilfeller gjør OED vurderingen og gir sikkerhetsklarering. Klareringsanmodningen skal gå via beredskapsseksjonen i NVE.

4.2.4 Henvisninger

Nasjonal sikkerhetsmyndighet (NSM) sin veiledning om sikkerhetsklarering kan lastes ned på www.nsm.stat.no

§4-3 Anskaffelser i kraftforsyningen

Leverandører som i forbindelse med oppdrag for kraftforsyningen kan få tilgang til sensitiv informasjon, skal inngå en sikkerhetsavtale med Norges vassdrags- og energidirektorat eller vedkommende enhet i KBO.

Ved oppdrag som medfører at leverandøren kan få tilgang til sikkerhetsgradert informasjon, skal anskaffelsen gjennomføres i samsvar med bestemmelser gitt i og i medhold av sikkerhetsloven.

Veiledning

Hensikten med bestemmelsen er å sikre at leverandører med tjenstlig behov som får tilgang til sensitiv informasjon (§§ 6-1 Generelt og 6-2 Beskyttelse av informasjon), eller sikkerhetsgradert informasjon (sikkerhetsloven, LOV 1998-03-20-10, § 11) behandler informasjonen etter gjeldende lover, forskrifter og interne sikkerhetsinstrukser. Med leverandører menes det i denne sammenheng alle som leverer varer, produkter, og tjenester til, eller har et oppdrag av relevans for kraftforsyningen. Dette inkluderer også lovbestemte oppdrag for statlige eller kommunale myndigheter.

Enheten kan dele sensitiv informasjon med andre KBO-enheter uten forutgående inngåelse av sikkerhetsavtale.

4.3.1 Sensitiv informasjon til leverandør - sikkerhetsavtale og taushetserklæring

Før en KBO-enhet gir en leverandør tilgang til sensitiv informasjon i henhold til § 6-2 Beskyttelse av informasjon, skal det inngås en sikkerhetsavtale med leverandøren (se Mal for sikkerhetsavtale på www.nve.no). Avtalen innebærer at leverandøren forplikter seg til å beskytte sensitiv informasjon om kraftforsyningen. Sikkerhetsavtalen og taushetserklæring signeres av daglig leder. Det bør etableres rutiner som sikrer slik forankring. Utførende personell skal signere taushetserklæring før de får tilgang til sensitiv informasjon. Taushetserklæringene oppbevares og administreres av firmaet selv.

NVE kan i enkelte tilfeller inngå sikkerhetsavtaler med landsomfattende leverandører til kraftforsyningen. Dette blir gjort for at leverandøren skal slippe å lage separate sikkerhetsavtaler med ulike KBO-enheter. NVE v/Beredskapsseksjonen har oversikt over leverandører som har en slik sikkerhetsavtale, og tar i mot henvendelser i forbindelse med spørsmål om dette, samt ønsker om nye sikkerhetsavtaler mellom NVE og leverandører. Dersom enheten bruker lokale leverandører, må enheten fortrinnsvis inngå egne sikkerhetsavtaler med disse leverandørene.

4.3.2 Sensitiv informasjon til selskaper i eget konsern som ikke er KBO-enheter

Dersom selskaper i et konsern som ikke er KBO-enheter har tjenestelig behov for sensitiv informasjon fra en KBO-enhet i konsernet, må enheten inngå en sikkerhetsavtale med det aktuelle selskapet på lik linje med andre eksterne selskaper.

4.3.3 Sikkerhetsgradert informasjon

Sikkerhetsgradert informasjon omfatter all informasjon som er merket med rødt stempel med sikkerhetsgrad, i henhold til sikkerhetsloven (LOV 1998-03-20-10). Reglene for tilgang til slik informasjon finnes i sikkerhetsloven kapittel 7 sikkerhetsgraderte anskaffelser. Utfyllende regler finnes i forskrift om sikkerhetsgraderte anskaffelser, (FOR-2001-07-01-753), og forskrift om informasjonssikkerhet, (FOR-2001-07-01-744).

Andre med tjenestelig behov for tilgang til sensitiv informasjon

I noen situasjoner kan aktører som verken er KBO-enheter eller leverandører ha tjenestelig behov for sensitiv informasjon. Eksempler på dette er kommersielle aktører i og utenfor Norge som ønsker å undersøke:

Tekniske og kommersielle muligheter for investeringer i vindkraft, småkraftproduksjon, eller liknende

Muligheter for tilførsel av elektrisitet fra fastlandet til offshoreinstallasjoner

Dette er ikke regulert i beredskapsforskriftens bestemmelser, og slike saker må vurderes enkeltvis av NVE. Saksgangen er da som følger:

Firmaet som har behov for innsyn, retter en skriftlig henvendelse til NVE med en kort beskrivelse av hva slags informasjon som ønskes utlevert, og hvilke nettselskaper det gjelder. Firmaet sender kopi til angjeldende nettselskap.

NVE oversender sikkerhetsavtale for underskrift, og taushetserklæring for bruk i angjeldende firma. Firmaet er selv ansvarlig for at egne medarbeidere som kan få tilgang til informasjonen, underskriver taushetserklæringen. Firmaet som mottar nettdataene har ikke anledning til å videreformidle mottatt informasjon.

Når NVE har mottatt undertegnet sikkerhetsavtale, gir NVE nettselskapet dispensasjon fra de relevante forskriftsbestemmelser slik at informasjonen kan utleveres.

Firmaet anmoder nettselskapet om utlevering av nettdata. Kopi av inngått sikkerhetsavtale med NVE vedlegges.

Nettselskapet kan deretter utlevere nettdata. Ved utlevering bør nettselskapet gi nødvendige vilkår for tilbakelevering eller sletting av dataene.

§4-4 Begrenset anbudsinnbydelse

En anbudsinnbydelse skal begrenses når det er nødvendig å hindre at sikkerhetsgradert eller annen sensitiv informasjon blir offentlig tilgjengelig gjennom anbudsdokumentene. Dette gjelder blant annet skjermingsverdige objekter i henhold til sikkerhetsloven og sensitiv informasjon etter denne forskrifts § 6-2.

Veiledning

Begrenset anbudsinnbydelse er i henhold til anskaffelsesregelverket en anskaffelsesprosedyre som bare tillater leverandører som er invitert av oppdragsgiver til å gi tilbud.

Dersom anbudsdokumentene eller oppdraget inneholder sensitiv informasjon, kan anbudet begrenses ved at kun leverandører som har inngått sikkerhetsavtale med NVE eller direkte med KBO-enheten, får tilsendt anbudsdokumenter.

For anskaffelser som innebærer utlevering av sikkerhetsgradert informasjon, vises det til sikkerhetsloven (LOV 1998-03-20-10) med forskrifter. Det vises forøvrig til forskrift om innkjøp i forsyningssektorene (FOR 2006-04-07-403).

§4-5 Adgangskontroll

Alle kraftforsyningsanlegg skal være sikret mot adgang for uvedkommende. Dette gjelder også øvrige bygg av betydning for kraftforsyningens ledelse og drift. Driftssentraler med tilhørende utrustning skal i tillegg defineres som egen adgangskontrollert sikkerhetssone.

Veiledning

Bestemmelsen vedrørende adgangskontroll gjelder for:

- Driftssentraler og rom med tilhørende utrustning.
- Bygninger og områder med kraftforsyningsanlegg.
- Kontorbygninger for drift og ledelse.
- Lagerområder ute og inne med beredskapslager og beredskapsrom.

Enheten kan etablere adgangskontroll ved avlåsing, vakthold, overvåking, registrering og/eller ved bruk av andre tekniske løsninger. Se også kapittel 5 Sikringstiltak og § 6-4 Særlige krav til driftskontrollsystemer.

Enheten bør innarbeide en rutine for å kontrollere at porter, dører og vinduer fungerer etter hensikten og lar seg lukke og låse. Enheten må ha god kontroll med tilgangsrettigheter for nøkkelkortsystemer. Der nøkkelkort brukes, bør det kombineres med krav om pin-kode for atkomst/tilgang. Alminnelige låsesystemer er sårbare for at nøkler mistes, og enheten må ha rutiner for administrering, slik at nøkler på avveie oppdages. Adgangskontrollsystemer som kan logge aktivitet er å anbefale. Slike logger bør gjennomgås jevnlig for å avdekke sikkerhetshendelser.

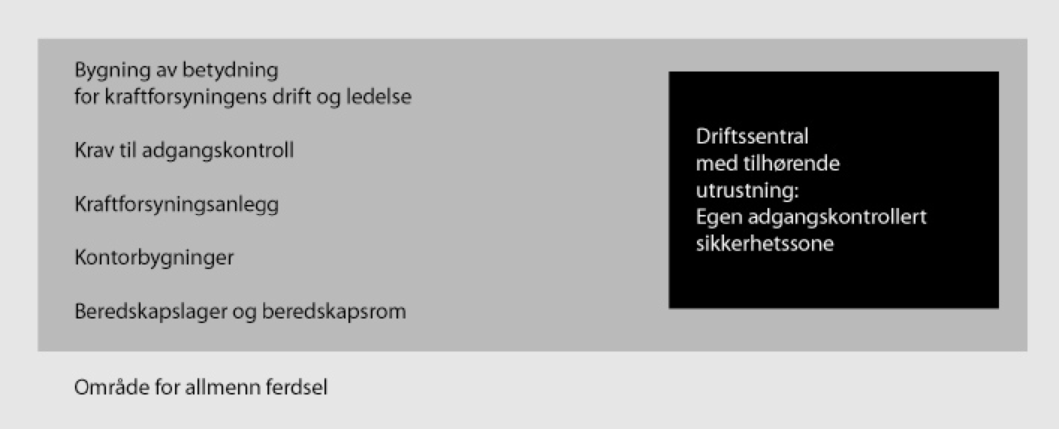
4.5.1 Krav til adgangskontroll til driftssentraler

Driftssentraler med tilhørende utrustning inkluderer:

- Driftssentraler, sambandsanlegg og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner.
- 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 styring av koblinger og overvåking av tilstand i anleggene.

Rom som inneholder driftssentraler med tilhørende utrustning skal være egne adgangskontrollerte sikkerhetssoner. Enheten må holde disse rommene avlåst for alle som ikke har selvstendig adgang. Personer kan få selvstendig adgang gjennom autorisering. Øvrige skal ledsages av personer som har gyldig autorisasjon. Dersom enheten har bærbart utstyr som kan brukes til styring og kontroll av kraftsystemkomponenter utenfor driftssentralen, for eksempel på eget kontor eller hjemmevakt, se 6.4.2.11 Fjerntilgang, hjemmevakt.

Sikkerhetssonen skal være utstyrt med adgangskontrollsystemer av en slik kvalitet at de ikke kan forseres uten at det foretas et synlig innbrudd. For ytterligere krav til sikring av driftskontrollsystemer, se § 6-4 Særlige krav til driftskontrollsystemer, punkt b. Tilgangskontroll. For veiledning om fysiske barrierer, se § 5-5 Sikringsnivå.



Figur 1: Prinsipp for adgangskontroll

4.5.2 Spesielle krav ved bygge- og installasjonsarbeid

I anleggsfasen må enheten etablere adgangskontroll senest fra det tidspunkt installasjonsarbeidene begynner. Alle faste adgangsberettigede skal utstyres med adgangskort. Tilfeldige arbeidstakere, leverandører, besøkende og liknende skal gis tidsbegrensede adgangskort. Kjøretøyer skal være registrert og ha parkeringstillatelse. For besøkende, se også § 4-6 Besøksrestriksjoner.

§4-6 Besøksrestriksjoner

Alle driftssentraler i klassifiserte driftskontrollsystemer, og alle kraftforsyningsanlegg klassifisert i klasse 3 etter denne forskrifts § 5-3, skal ha besøksrestriksjoner. Norges vassdrags- og energidirektorat kan vedta at kraftforsyningsanlegg i klasse 2 også skal ha besøksrestriksjoner.

Ved anlegg underlagt besøksrestriksjoner skal:

a) de besøkende følge en fast avgrenset rute,

b) de besøkende til enhver tid være ledsaget av en erfaren og ansvarlig representant for anleggets eier,

c) det ikke gis opplysninger om sensitive forhold,

d) det ikke gis detaljerte opplysninger om anleggets oppbygning, drift eller lignende forhold,

e) fotografering være forbudt med mindre spesiell tillatelse er innhentet fra anleggets eier.

Studieopphold og praktikanttjeneste ved anlegg underlagt besøksrestriksjoner kan utføres av norske statsborgere. Norges vassdrags- og energidirektorat kan etter søknad gi tillatelse til studieopphold og praktikanttjeneste for utenlandske statsborgere.

Eier av anlegg underlagt besøksrestriksjoner skal utarbeide instruks for besøk.

Veiledning

4.6.1 Kontroll med besøk

For å motvirke tilsiktede uønskede hendelser og handlinger eller forberedelser til slike, skal følgende viktige kraftforsyningsanlegg ha besøksrestriksjoner:

- Alle anlegg i klasse 3.
- Anlegg i klasse 2 hvor NVE har fattet enkeltvedtak.
- Alle klassifiserte driftssentraler (inklusive relevante IT- og sambandsanlegg).

Ved ovennevnte anlegg kan eier eller ansvarlig driftsselskap ha kortvarige kontrollerte besøk. Det skal være tungtveiende informasjonsfaglige grunner for besøket. Ukontrollerte turistbesøk uten tjenestelige behov er ikke tillatt.

4.6.2 Besøkets begrensninger

- Besøket skal følge en fast avgrenset rute og til enhver tid være ledsaget av en ansvarlig representant for anleggets eier. Ledsagere må kjenne anlegget, beredskapsforskriftens krav, lokal instruks for besøk, og kunne påse at disse og andre krav til sikkerhet blir overholdt
- For at ledsageren til enhver tid skal ha nødvendig oversikt over de besøkende, bør besøket avgrenses både i antall, tid og rom. Antallet besøkende bør begrenses til det antallet ledsageren til enhver tid kan ha oppsyn med, og tiden bør avgrenses til maksimalt to timer
- Ruten bør være avgrenset til de delene av anlegget hvor ledsageren lett kan føre kontroll med besøkende, og hvor det er lite sensitiv informasjon. Om nødvendig avmerkes/separeres tillatt og ikke tillatt område
- Enheten bør unngå kjøring i anlegget. Dersom kjøring er nødvendig, skal dette fortrinnsvis skje med eiers egne kjøretøyer. Det er ikke tillatt å la ukjente kjøretøyer kjøre i anlegget.

4.6.3 Identifikasjon og besøkslister

For å hindre adgang for uvedkommende og ivareta sikkerheten (også personsikkerheten) bør alle besøkende identifiseres. Besøkende bør vise godkjent og gyldig identifikasjon med bilde, navn, nasjonalitet, fødselsdato og underskrift. For utenlandske statsborgere utenfor Norden vil dette bety pass eller EU-godkjent identifikasjon. Personer uten identifikasjonspapirer bør ikke gis adgang. Unntak kan gjøres for eksempel ved besøk av en lokal skoleklasse eller andre velkjente personer som eier kan gå god for.

Før besøket i anlegget bør det utarbeides en liste med alle de besøkendes navn, nasjonalitet og fødselsdato. Listen bør oppbevares i minimum 5 år etter besøket.

4.6.4 Sensitiv informasjon

Under besøket skal ikke enheten spre sensitiv informasjon, se også §§ 6-1 Generelt og 6-2 Beskyttelse av informasjon. Enheten kan ikke gi detaljerte opplysninger om anleggets oppbygning, drift eller lignende forhold.

4.6.5 Forbud mot fotografering og medbringing av gjenstander

Fotografering er forbudt, med mindre spesiell tillatelse er innhentet fra anleggets eier og sikkerhetsmessige forhold er tatt hensyn til. For å håndheve forbudet effektivt er det normalt ikke tillatt å ha med seg gjenstander inn i anlegget som kan ta bilder og/eller film. Det bør ikke være tillatt å ta med noen gjenstander inn i anleggets sentrale og vitale deler, også av risiko for eksempelvis medbrakte eksplosiver, jamme- eller avlyttingsutstyr.

4.6.6 Eiers inviterte gjester

Det kan være aktuelt for eier å invitere besøkende med et faglig rettmessig informasjonsbehov, eksempelvis bransjefolk og studenter. Dersom dette er personer eieren av anlegget kan gå god for, kan enheten gjøre unntak fra ovennevnte begrensninger, men enheten må da utvise sikkerhetsmessig aktsomhet.

4.6.7 Studie- og andre liknende opphold

Ved studie- og andre liknende opphold er det en forutsetning at anleggets eier/driftsansvarlig legger til rette for, og har tett oppfølging av alle sikkerhetsforhold. Ved besøk av utenlandske statsborgere må enheten alltid kontakte NVE ved Beredskapsseksjonen i god tid på forhånd. Dersom studenten(e) utfører oppdrag eller tjenester, gjelder også de andre bestemmelsene i kapittel 4.

4.6.8 Instruks for besøk

Instruks for besøk må minst omfatte følgende:

- Kravene som stilles i denne bestemmelsen.
- Begrensninger beskrevet i veiledningen til dette kapittelet.
- Kravene i beredskapsforskriften for øvrig.
- Forhold som kommer frem av ROS-analysene.

4.6.9 Driftssentraler i driftskontrollsystemer klasse 3

Besøk skal normalt ikke være tillatt i driftssentraler i klasse 3. Det er bare personer med tjenestelig behov som skal gis adgang. Besøksinstruksen bør beskrive hvilke myndigheter og øvrige enheter som man forventer kan ha tjenstlig behov for adgang, og hvordan disse skal ledsages. Forøvrig skal det generelle besøksforbudet være stadfestet i besøksinstruksen.

4.6.10 Henvisninger

Enkeltvedtak av 29.06.2006: Besøksrestriksjoner og adgangskontroll ved kraftanlegg. Presisering av bestemmelser i beredskapsforskrift for kraftforsyningen, se vedlegg.

Kap 5 Sikringstiltak

Bestemmelsene i kapittel 5 inneholder regler om sikringstiltak for anlegg.

Eier av et anlegg plikter å melde fra om bygging og vesentlige endringer til NVE, etter § 5-2 Meldeplikt

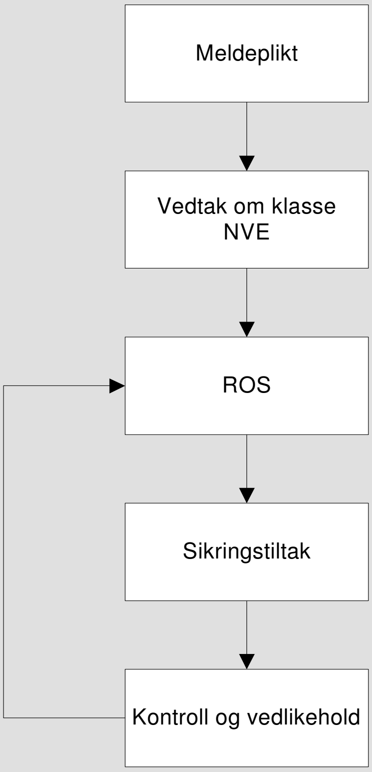
NVE vedtar deretter anleggets klasse etter fastsatte kriterier, se § 5-3 Klassifisering

Med bakgrunn i NVE sitt vedtak om klasse skal KBO-enheten utarbeide en ROS-analyse for anlegget, §§ 5-4 Analyse og 1-3 Risiko- og sårbarhetsanalyse. Denne analysen skal bidra til å sikre en rasjonell etterlevelse av de funksjonelle kravene som er gitt i § 5-5 Sikringsnivå.

Enheten skal implementere nødvendige sikringstiltak, herunder gjennomgå og oppdatere gamle og supplere med nye sikringstiltak etter §§ 5-5 Sikringsnivå og 5-6 Vakthold.

§ 5-7 Kontroll og vedlikehold stiller krav om jevnlig kontroll og vedlikehold av alle sikringstiltak på anlegget, både aktive og passive.

Enheten må revidere analysen jevnlig og ha et kvalitetssystem som sikrer dette, se §§ 5-4 Analyse, 1-3 Risiko- og sårbarhetsanalyse og 1-2 Kvalitetssystem.



Figur 2: Prosessen med sikring av anlegg etter § 5

§5-1 Sikringsplikt

Alle anlegg som omfattes av energilovforskriften § 8-3 skal være sikret mot uønskede hendelser og handlinger.

Veiledning

Alle eiere og drivere av kraftforsyningsanlegg har en selvstendig plikt til å vurdere og iverksette sikringstiltak etter denne forskriften ved de kraftforsyningsanleggene selskapet har ansvar for.

Bestemmelsen fastsetter en alminnelig sikringsplikt for alle kraftforsyningsanlegg som omfattes av energilovforskriften § 8-3. Disse anleggene er nærmere definert i § 5-2 Meldeplikt. Bestemmelsen har størst praktisk betydning for kraftforsyningsanlegg i klasse 1, eller anlegg som av ulike grunner er uklassifisert. Krav til sikringstiltak på klassifiserte anlegg er gitt i § 5-5 Sikringsnivå.

Dersom anlegget ikke er klassifisert, står eier relativt fritt til å vurdere hvilke sikringstiltak som skal gjennomføres. Det forutsettes uansett en dokumenterbar vurdering etter § 1-3 Risiko- og sårbarhetsanalyse, som tar hensyn til stedlige forhold og risiko. De mest relevante risikomomentene i en generell risiko- og sårbarhetsanalyse for alle anlegg vil være sikring mot innbrudd, hærverk, brann og naturskade. Det må være en fornuftig balanse i sikringstiltakene. Det er for eksempel begrenset virkning av en solid dør dersom usikrede vinduer på bakkeplan gir adkomst til samme arealer.

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

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

5.1.1 Henvisninger

- Lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver (brann- og eksplosjonsvernloven) av 14 juni 2002, med forskrifter - bl.a.
- Forskrift om brannforebyggende tiltak og tilsyn (Forebyggendeforskriften), fastsatt av Direktoratet for samfunnssikkerhet og beredskap (DSB) 26 juni 2002.

- ”Temaveiledning – brannvern i kraftforsyningen”, Direktoratet for samfunnssikkerhet og beredskap (DSB) og Norges vassdrags- og energidirektorat (NVE), november 2003.
- Lov om planlegging og byggesaksbehandling (plan- og bygningsloven) av 27 juni 2008, med forskrifter – bl.a.
- Forskrift om tekniske krav til byggverk (Byggteknisk forskrift) av Kommunal- og regionaldepartementet, 26 mars 2010
- "Forskrift om elektriske forsyningsanlegg" (FEF) fastsatt av DSB 20. desember 2005, i kraft 1. januar 2006 med hjemmel i lov 24. mai 1929 nr. 4 om tilsyn med elektriske anlegg og elektrisk utstyr. Veiledning til FEF fastsatt av DSB – bl.a. Kapittel 4 Høyspenningsinstallasjoner.
- ”Forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg” (FSE), fastsatt av 28. april 2006 med hjemmel i lov 24. mai 1929 nr. 4 om tilsyn med elektriske anlegg og elektrisk utstyr.
- ”Forskrift om objektsikkerhet”, fastsatt ved kgl.res. 22. oktober 2010 med hjemmel i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven). Det gjøres samtidig oppmerksom på at sektorbestemmelser som Beredskapsforskrift for kraftforsyningen går foran denne forskrift.
- ”Forskrift om behandling av personopplysninger” (personopplysningsforskriften), Fastsatt ved kgl.res. 15. desember 2000 med hjemmel i lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
- Lov om petroleumsvirksomhet (petroleumsloven) av 29. november 1996 med forskrifter, er relevant for bl.a. gassdrevne kraftverk.

For krav til innbrudds- og hærverkssikring kan enheten ta utgangspunkt i kravene om Forsikringsselskapenes Godkjennelsesnemnd (FG) setter til relevante dører, porter, vinduer og lignende med innfesting, karmer og låseanordninger. Her vises det også til gjeldende Europeiske normer, se veiledning under §5-5 Sikringsnivå.

§5-2 Meldeplikt

Eiere av eksisterende og planlagte kraftforsyningsanlegg som omfattes av energilov-forskriften § 8-3 – i henhold til energiloven § 9-6, skal melde fra til Norges vassdrags- og energidirektorat i god tid før arbeidet settes i gang.

Slike meldinger om bygging, utvidelser, ombygging med videre av anlegg, skal være bilagt de dokumenter som er nødvendig for at vedtak om sikringsnivå kan treffes.

Veiledning

Det er fastsatt en meldeplikt i energiloven § 9-6 for den som vil bygge, bygge om, endre eller utvide anlegg som omfattes av energiloven § 9-3 Sikringstiltak[1]. Enheten skal melde fra til NVE i god tid før arbeidet settes i gang.

Beredskapsseksjonen ber om å få meldingen tilsendt minimum 6 måneder før anleggsstart. Meldingen må komme i tilstrekkelig tid til at NVE får behandlet meldingen og fastsatt klasse etter § 5-3 Klassifisering, og til at eier får:

---

[1] Tidligere § 6-6 og § 6-3

- Foretatt ROS-analyser.
- Implementert alle følgende krav til sikringstiltak etter §§ 5-4 Analyse og 5-5 Sikringsnivå.

Ovennevnte punkter bør gjøres som en integrert del av planprosessen. Dersom eventuelt anbud skal begrenses (se § 4-4), må enheten ta kontakt med NVE før anbud sendes ut.

Meldeplikten omfatter følgende anlegg:

- Kraftverk med generatoreffekt på minst 15 MVA. Dette gjelder kraftstasjonens samlede generatoreffekt, selv om denne er fordelt på flere generatorer, uavhengig av energikilde.
- Transformator- eller koblingsstasjon med gjennomgangseffekt på minst 10 MVA og omformerstasjon med gjennomgangseffekt på minst 2 MVA. Med omformerstasjon forstås all omforming av elektrisk kraft, også strømretteranlegg. Omformerstasjoner for jernbane og sporvei er unntatt meldeplikt.
- Elektrisk kraftledning beregnet på minst 132 kV nominell spenning. Kraftledninger er inntil videre unntatt meldeplikt. Klassifisering av kraftledninger er til vurdering i NVE.
- Damanlegg eller andre reguleringsanlegg som kan magasinere minst 5 millioner kubikkmeter vann. Slike anlegg skal ikke meldes etter denne paragrafen, idet de klassifiseres under vassdragslovgivningen - blant annet forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften) FOR-2009-12-18-1600.
- Fjernvarmeanlegg som har en ytelse på minst 10 MJ/s. Dette gjelder et fjernvarmeanleggs samlede installerte ytelse.
- Driftssentraler. Med driftssentral regnes her også sambandsinstallasjoner og lignende som er nødvendige for kraftsystemets driftskontrollfunksjoner, se § 6-4 Særlige krav til driftskontrollsystemer. Det skal sendes inn melding hvor hele driftskontrollsystemet ses under ett.

Når særlige forhold tilsier det, kan NVE vedta at også anlegg som ikke fyller ovennevnte minstekrav skal meldes til NVE. Dette kan eksempelvis gjelde anlegg som forsyner særlig viktige installasjoner.

Vindmølleparker meldes som kraftverk når samlet generatoreffekt overstiger 15 MVA. I slike tilfeller kan parken ha en egen transformatorstasjon der gjennomgangseffekten er over 10 MVA. Det er hensiktsmessig å melde vindmølleparken og transformatorstasjonen samlet.

5.2.1 Nærmere om meldeplikten

Etter ovennevnte punkter skal nye anlegg alltid meldes til NVE. Enheten kan gjerne sende inn meldingen sammen med konsesjonssøknaden, men endelig vedtak om klasse kommer ikke før konsesjon er gitt. I henhold til bestemmelsene i kapittel 5 sikringstiltak og § 7.2 a overtredelsesgebyr, anbefales enheten å vente med byggestart til klassifisering av anlegget foreligger.

Enheten skal også melde inn vesentlige endringer i eksisterende anleggs funksjon eller kapasitet til NVE. For mindre vesentlige endringer skal enheten kun informere NVE om tiltak som planlegges utført, og når anlegget er ferdigstilt, etter § 5-4 Analyse.

Eksempler på endringer som utløser meldeplikt:

Anleggets kapasitet endres med 50 % eller mer

Driftssentral som overtar styring av tilsvarende flere anlegg målt i ytelse

Enheten ser at endringer kan føre til klasseendring for anlegg

Eksempler på endringer som ikke utløser meldeplikt, men som utløser informasjonsplikt etter § 5-4:

Økning av ytelse i et anlegg som allerede er i klasse 3

Endringer som nødvendiggjør ombygninger som inkluderer sikringstiltak

Eksempel på endring som verken utløser meldeplikt, eller informasjonsplikt etter § 5-4:

Utskifting av anleggsdeler med mindre enn 50 % endring i kapasitet uten vesentlige endringer i sikringstiltak

Dersom endringene ikke utløser meldeplikt, skal sikringstiltak vurderes, utføres og dokumenteres av enheten selv.

Ta kontakt med NVE ved Beredskapsseksjonen dersom det er tvil om en endring utløser meldeplikt etter denne paragrafen eller informasjonsplikt etter § 5-4 Analyse.

Alle meldinger skal inneholde:

- Utfylt meldingsskjema, som kan lastes ned på www.nve.no.
- Vedlegg i form av planer, beskrivelser, tegninger og kart som er nødvendige for at vedtak kan treffes.

Meldingen skal sendes til NVE, Beredskapsseksjonen. Utfylt skjema vil normalt være underlagt taushetsplikt etter § 6-2 Beskyttelse av informasjon og unntatt offentlighet etter offentleglova § 13 første ledd.

§5-3 Klassifisering

Norges vassdrags- og energidirektorat vedtar klassifisering av anlegg som nevnt i energilovforskriften § 8-3 i tre klasser etter sin betydning for landets kraftforsyning.

a) Klasse 1

Anlegg av mindre betydning.

b) Klasse 2

Anlegg som har betydning for opprettholdelse av kraftforsyningen på fylkesnivå eller for drift av regionalnett.

c) Klasse 3

Anlegg som har betydning for kraftforsyningen i en landsdel, region eller for drift av sentralnettet eller for store befolkningsgrupper, viktig infrastruktur eller andre særlige hensyn.

Veiledning

Etter at enheten har meldt til NVE om planlagte anlegg eller vesentlige endringer ved eksisterende anlegg etter § 5-2 Meldeplikt, vil NVE vedta en klasse for det innmeldte anlegget ut fra en vurdering av ulike forhold.

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

For fjernvarmeanlegg klassifiseres hver enkelt varmesentral for seg, eller hele systemet under ett, med tilhørende driftskontrollsystem.

§5-4 Analyse

Eier skal på bakgrunn av Norges vassdrags- og energidirektorats vedtak om klasse foreta egen risiko- og sårbarhetsanalyse (ROS), samt planlegge og utføre anleggene og systemene som angitt i denne forskriften. Norges vassdrags- og energidirektorat skal informeres om de tiltak som planlegges utført, og når anlegget er ferdigstilt.

Veiledning

I følge § 1-3 om risiko- og sårbarhetsanalyser, skal enheten utarbeide en risiko- og sårbarhetsanalyse (ROS-analyse) for enheten som helhet.

§ 5-4 stiller et spesifikt krav om at enheten skal utarbeide egne ROS-analyser for hvert av sine klassifiserte anlegg. Hensikten med dette er at enheten skal tilrettelegge sikringen av sine klassifiserte anlegg etter lokale forhold, som eksempelvis risiko for flom og skred.

Dette analysekravet gir ikke enheten anledning til å velge løsninger som er svakere enn det grunnsikringsnivået som følger av kravene i beredskapsforskriften, se særlig § 5-5 Sikringsnivå.

ROS-analysene skal inkludere alle uønskede hendelser som kan ramme anleggene i forhold til naturgitt skade, teknisk svikt og tilsiktede ødeleggelser. Analysen skal først og fremst vurdere sårbarhet og uønskede konsekvenser. Fokuset bør være på sikring av ledelse og drift, samt mulig skade på kraftforsyningsanlegg. Dette gjelder også driftskontrollsystemer og sambandsanlegg. Enheten må analysere alle uønskede hendelser innenfor ovennevnte kategorier, selv om sannsynligheten kan virke liten.

I en analyse av risiko for bevisst skadeverk skal det tas hensyn til bruk av hjelpemidler med både lett og begrenset tilgjengelighet. For anlegg i klasse 3 må analysen også dekke mulig bruk av hjelpemidler som i utgangspunktet er lite tilgjengelige.

5.4.1 Planlegge og utføre anlegg og systemer

På grunnlag av § 5-5 Sikringsnivå, deles sikringstiltakene inn i:

- Grunnsikring.
- Forberedt tilleggssikring.

Enheten skal derfor planlegge og utføre sine anlegg og systemer etter følgende prinsipper:

- Tilpasse grunnsikringen til lokale forhold.
- Vurdere og forberede tilleggssikring.

Alle vurderinger enheten gjør, samt tiltak enheten iverksetter, skal dokumenteres, i henhold til § 1-2 om kvalitetssystem.

5.4.2 Informasjonsplikt

Enheten har etter siste punkt i denne bestemmelsen plikt til å informere NVE om de tiltak som planlegges utført, og når anlegget er ferdigstilt.

Først etter klassifiseringen og gjennomføring av ROS-analysen er det fullt ut mulig å planlegge de nødvendige sikringstiltak. En oversikt over de planlagte tiltak skal sendes NVE. Dette gir selskapene og NVE en mulighet for å vurdere tiltakene før de iverksettes eller bygges. Etablering av/eller endring av sikringstiltak etter at anlegget er bygd, er ofte mer komplisert og kostbart.

Når anlegget er ferdigstilt, skal NVE informeres særskilt om dette.

§5-5 Sikringsnivå

Kraftforsyningsanlegg skal etter sin klasse oppfylle følgende krav til sikring:

a) Klasse 1
Anlegget kan i alminnelighet utføres med enkle krav til sikringsnivå. Funksjonstap skal kunne gjenopprettes innen rimelig tid.

b) Klasse 2
Anlegget skal være utført og utstyrt etter middels høye krav til sikring. I ekstraordinære situasjoner skal tap av vitale funksjoner begrenses og etter eventuell skade skal anleggets funksjonalitet kunne gjenopprettes innen rimelig tid.
Anleggets sikringsnivå skal være en kombinasjon av blant annet følgende tiltak:

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

2. Fysisk utførelse og beskyttelse skal være på et nivå som begrenser tap av funksjon og ødeleggelse.

3. Gjenoppretting av eventuelle funksjonstap skal skje innen rimelig tid.

4. Redundans i anlegget eller kraftsystemet
Anlegget skal fungere uavhengig av de strømutfall som kan forekomme i ordinær strømforsyning og påregnelige feil i eget strømforsyningssystem.
Anlegget skal kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriftens § 3-4.

c) Klasse 3
Anlegget skal være utført og utstyrt etter høye krav til sikring. Vitale funksjoner skal opprettholdes i ekstraordinære situasjoner og raskt gjenopprettes etter eventuell skade.
Anleggets sikringsnivå skal være en kombinasjon av blant annet følgende tiltak:

5. Alle uønskede hendelser og handlinger skal oppdages straks og håndteres av et effektivt reaksjonsmønster.

6. Fysisk utførelse og beskyttelse skal være på et nivå som forebygger eller forhindrer tap av funksjon og ødeleggelse.

7. Gjenoppretting av eventuelle funksjonstap skal skje straks.

8. Redundans i anlegget eller kraftsystemet.

Anlegget skal fungere uavhengig av ordinær strømforsyning og feil i anleggets eget strømforsyningssystem. Funksjon skal opprettholdes også ved upåregnelige og langvarige strømutfall.
Alle anlegg skal samtidig og innen rimelig tid kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriftens § 3-4.

Veiledning

5.5.1 Funksjonelle kriterier, hva skal oppnås

Hovedhensikten med denne bestemmelsen er at kraftforsyningsanlegg skal sikres mot skade som skyldes naturgitte forhold, teknisk svikt eller tilsiktede ødeleggelser i fred, under beredskap og krig – herunder:

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

Av hendelser som det må være sikringstiltak mot, er:

- Inntrengning av uønskede personer og ytre skadeverk (inkludert håndvåpen, splinter og EMP).
- Naturskade (hvor relevant) som ras (jord, stein, snø), steinsprang, flom/oversvømmelse, belastninger fra nedbør og uvær, snø, is og atmosfæriske forstyrrelser.
- Utilsiktede hendelser som kan forårsake tap av vitale funksjoner.

Krav til sikringstiltak er avhengig av anleggenes klassifisering etter § 5-3, og kravene øker med klasse.

Sikringstiltak består av fire ulike kategorier tiltak:

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

Kategoriene kompletterer hverandre. Alle fire må derfor alltid være til stede, i større eller mindre grad.

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

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

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

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

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

Det forutsettes at krav til rømningsveier oppfylles, og at disse tilrettelegges og utføres slik at oppfyllelse av BfKs krav til sikringstiltak ikke er til hinder for dette - f.eks.:

- avstengte anleggsdeler kan åpnes når det er personell til stede i anlegget.
- innvendige åpningsanordninger må ikke kunne åpnes eller manipuleres utenfra.

Selskapene skal kunne dokumentere at de krav som gis i § 5-5 i sum er oppfylt.

Mer detaljerte beskrivelser av krav til, og utforming av, sikringstiltak (skallsikring og lignende ved de enkelte typer anlegg etter klasse) er gitt i vedlegg til denne veiledningen. Dette vedlegget er underlagt taushetsplikt etter BfK § 6-2 og unntatt offentlighet etter offentleglova § 13, 1. ledd.

Henvisning til normer og standarder

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

I denne paragrafen om sikringsnivå henvises til en del gjeldende normer om brannvern, konstruksjoner og beskyttelse mot inntrengning, først og fremst til nye europeiske norm EN. Det finnes imidlertid ekvivalenter etter norsk standard (NS), selv om noen av disse nå er utgått. Også svensk og internordisk standard er en del brukt på nevnte områder. Det finnes derfor en rekke normer for ulike områder og produkter. De nordiske forsikringsforbund har med tanke på bl.a. innbruddssikring med videre utarbeidet en ”Sammenligningsnøkkel”. Denne og forklaring til normer for sikring og sikkerhet kan søkes opp på hjemmesidene til ”Forsikringsselskapenes Godkjennelsesnemnd (FG): [http://fg.fnh.no/]. Også Direktoratet for samfunnssikkerhet og beredskap henviser til ulike relevante normer i deres regelverk og publikasjoner [http://www.dsb.no/].

I det norske marked kan det være en utfordring å få leverandører og relevante produkter som er sertifisert etter de her nevnte normer. Formålet med henvisningen til standarder er også å vise hvor nivået skal ligge for ulike produkter. Ekvivalenter som tilsvarer de nevnte normer kan godtas.

For låssystemer er det også vist til ”Forsikringsselskapenes Godkjennelsesnemnd” (FG), godkjenningsklasse, siden dette er et oversiktlig system å forholde seg til med mange godkjente produkter på markedet.

For elektroniske/ elektromekaniske låssystem har FG (se http://fg.fnh.no/) nylig (mars 2010) utgitt en publikasjon med krav til slike. Disse er inndelt i 3 beskyttelsesklasser hvorav B2 og B 3 har mekanisk tilleggslås. Både av hensyn til inntrengingssikkerhet og egen tilgjengelighet til bygg og anlegg, er det B2 og B3 som er relevante i kraftforsyningen; B3 for anlegg i klasse 3.

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

De fleste sikringsstandarder (f.eks. mot innbrudd) etter EN har skala fra sikringsklasse 1 til 6. Denne veiledningen starter her på sikringsklasse 3 som f.eks. for en entrèdør (leilighet) tilsvarer normal innbruddssikring etter ENV 1627. Tilsvarende starter veiledning på FG klasse 2, siden FG klasse 1 er beregnet for ”redskapsboder” o.l.

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

Se punkt 5.5.10 for en beskrivelse av hvordan NVE vil praktisere forskriftens bestemmelser om sikringstiltak for hhv. nye kraftforsyningsanlegg, eksisterende anlegg som skal bygges om, eller utvides, og øvrige eksisterende anlegg.

5.5.2 Forebygge og forhindre tap av funksjon og ødeleggelse

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

- Hensikten med disse bestemmelsene er primært å hindre uvedkommende i å utføre tilsiktede handlinger rettet mot kraftforsyning. I forhold til DSBs bestemmelser om elsikkerhet vil beredskapsforskriften stille høyere krav, aldri lavere.

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

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

Når det gjelder plassering av nye kraftforsyningsanlegg, må enheten i sin risikovurdering vektlegge blant annet utsatthet for naturgitt skade, nærhet til utsatte objekter (storulykkepotensiale, risiko for transportulykker, tilgang ved reparasjon etc.). Dette er også forhold som skal vurderes i forbindelse med konsesjonssøknader. Se Veileder for utforming av søknad om anleggskonsesjon for kraftledninger, jord- og sjøkabler, transformatorstasjoner og elektriske anlegg i vannkraftverk.

Nedenfor beskrives nærmere krav til de enkelte typer av anlegg. Enheten kan finne alternative måter å løse kravet på, men dette må kunne dokumenteres. Eventuelle unntak, for eksempel ved at dette ikke passer for et gitt anlegg, skal begrunnes og dokumenteres.

For anlegg i klasse 1 gjelder krav til solid bygg etter vanlig byggestandard og eventuelt inngjerding dersom det er ytre anleggsdeler (friluftsanlegg). Disse må minst sikres etter moderate krav til standard/ norm for sikringsklasse. Etter FG blir dette klasse 2 eller 3. Etter for eksempel ENV 1627 og EN 12320 blir dette sikringsklasse 3 eller 4.

For anlegg i klasse 2 og 3 gjelder krav til

Skallsikring omfatter blant annet bygningskropp, transformatorceller med stengsler, ståldører og rister, kraftverksport (stål). Det må bygges og sikres etter middels eller høye krav til standard/norm for sikringsklasse. Etter FG må dette minst være i sikringsklasse 4, mens det etter ENV 1627 og EN 12320 blir minst sikringsklasse 5. Tilsvarende innbruddshemmende glass etter EN 356. Det må gis særlig oppmerksomhet mot svake punkter som vinduer, dører, kabelføringer og andre mulige atkomster.

Sonesikring innvendig av særlige viktige områder som kontrollrom, prosessmaskin/ sambandsrom, nødstrøm og lignende. Sikringsnivå tilpasses viktigheten av utstyret i sonen og nivået på ytre skallsikring, normalt FG-klasse 3 og sikringsklasse 3 eller 4 etter ENV 1627.

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

- Låser med tilhørende beslag og innfesting må for klasse 2-anlegg minst tilsvare FG klasse 2 med tilsvarende soliditet i port, bom og lignende i en balansert helhet, uten glipper og [særlig] svake punkter.
- Ofte vil for eksempel en transformator i klasse 2 stå i tett urban bebyggelse, og det kan da være umulig eller lite ønskelig eller hensiktsmessig å etablere fullverdig områdesikring. I tettbebygde områder, eller når andre særlige hensyn tilsier det, kan områdesikringen tillempes, men må da kompenseres ved andre tiltak (bedre skallsikring og liknende).
- Ved kraftstasjon klasse 2 vil det være naturlig å sette opp veibom og liknende, men det er ikke noe krav at portalbygg og liknende skal gjerdes inn dersom skallsikringen er tilfredsstillende.
- Alle kraftforsyningsanlegg i klasse 3 skal ha effektiv omsluttende områdesikring rundt viktige anleggsdeler, med mindre særlige forhold i omgivelsene tilsier noe annet.
  - **Bommer**. Der forholdene tilsier dette, sikres kjøreatkomster med solid veibom i passe avstand fra kjøreport. Bommen bør kunne låses med lås og beslag i sikringsklasse 3 eller 4. Omkjøring av bom vanskeliggjøres med grøfting eller kjøretøyavvisere.
  - **Gjerder**. Gjerder må være høye og solide. Høyden på gjerdet bør være på minst 2,7 meter.[2] Gjerdet (stolpene) må være solid fundamentert, støpt eller liknende i løs grunn, nedboret i fjell. Utstyres med solid og stram topp og bunntråd, eventuelt vinkeljern eller liknende, godt festet i stolpene. Gjerdedukens maskevidde (flettverksduk) maksimalt 50 millimeter og trådtykkelse min 2,8 millimeter. Gjerdeduken må være godt festet i både topp-/ bunntråd og i gjerdestolpene, både med tilstrekkelig antall og solide festetråder. Alle skjøter i gjerdetråd og duk må være godt sikret/sammenføyd. Glipper i/under gjerdet må ikke forekomme.
  - **Gjerdeporter**. Gjerdeporter (gang og kjøre/transport) må være solide med høyde og utførelse minst like bra som gjerdet. Stolper må støpes i løs grunn, bores ned eller boltes i fjell. Glipper må være minimale. Kjøreporter som skal beskytte kjøreatkomst mot innbrudd og inntrengning fra kjøretøy gis solid utførelse. To-fløyede porter må ha låsbar midtsikring mot bakke.
  - Styresystemet til elektrisk eller liknende drevne, eventuelt fjernstyrte porter må ikke kunne manipuleres utenfra eller via åpninger i port eller gjerde. Disse må også låses mekanisk (se under).
  - Portene må være utstyrt med låser og beslag sikringsklasse 3 eller 4, og bakkantbeslag eller hengsler sikret mot avløfting.
  - Der forholdene tillater dette, bør områdesikring settes opp i en avstand på minst 30 meter (”kasteavstand”) fra vitale komponenter.
  - Alle elementer i områdesikring bør holdes fri for vegetasjon, bygningselementer og andre gjenstander i en sone på 3 meter til alle kanter.
  - Alle løse gjenstander (for eksempel stiger, søppeldunker, kabletromler, hengere) som kan medvirke til enkel forsering av områdesikring skal normalt

---

[2] Det forutsettes i tillegg alltid vurdert anretning på toppen av gjerdet som ytterligere forebygger uønsket adkomst til området. Gjerde utføres evt. som stålstendere eller strekkmetall.

være plassert på innsiden, helst ute av syne, innelåst (alle verdigjenstander) eller fastlåst.

- Alle monteringselementer (eksempelvis låser, beslag, bolter, skruer) skal være sikret mot enkel demontering (av-/oppskruing).

NB! For eksisterende anlegg vises til veiledningens punkt 5.5.10.

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

Eksempler på ytterligere tiltak

Gjerdet forsterkes eller bygges høyere pga. snødybder, terreng, vegetasjon og omgivelser forøvrig.

Øvrige elementer som stolper, topp, bunn og innfesting forsterkes tilsvarende.

Montering av deteksjonsutstyr/-alarmer i ulike atkomster og innvendige rom. Forsterket overvåkning av funksjoner.

Forsterkning av gjerder og porter, bommer i kjøreatkomst og bakveier om nødvendig supplert med permanente stengsler/hindre som betongskillere eller store stein, forsterkede låser og beslag (høyere FG/sikringsklasse).

Ekstra krav til dører og porter, kraftverksdør/kraftverksport, ekstra kraftverksport, innbruddssikre vinduer og lignende, ekstra sikring av kabel og ventilasjonssjakter. Skuddsikre glass i kontrollrom, intern dublering av viktige funksjoner så som samband, nødstrøm og andre funksjoner.

For sonesikring – høyere sikringsklasse på dører, låser mv. eller ekstra brannsikring.

Ekstra inngjerding av vitale komponenter.

KBO-enheten har ansvaret for gjennom lokale analyser etter § 5-4, å sørge for at det blir et balansert og helhetlig sikringsnivå tilpasset anlegget.

I tillegg må planlagt/forberedt tilleggssikring kunne iverksettes ved behov. I en beredskapssituasjon må det for eksempel være supplerende sikrings- og beredskapstiltak som styrker beskyttelsen av vitale installasjoner og anleggsdeler mot for eksempel sabotasje. Dette kan skje ved varsel eller vedtak fra NVE eller overordnet myndighet, eller på enhetens eget initiativ ved en akutt oppstått situasjon.

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

Eksempler på planlagte og forberedte sikringstiltak

- Ekstra bemanning, forsterket vakthold, hyppigere inspeksjoner, ekstra låser og innskjerpede krav til tilgjengelighet og utrykningstider for personell.
- Reparasjonsberedskap gjennomgås, materiell klargjøres og suppleres.
- For fysisk områdesikring – porter forsynes med ekstra/dobbel lås, kjøreatkomster sperres med betongskillere, store steiner eller liknende, ekstra lyskastere settes ut. Kjetting med hengelås begge FG klasse 3 eller 4 for dobbel sikring av porter o. l. Kjøretøyavviser (stein, betong).
- For skallsikring – ekstra ståldører låses, stållemmer/skodder for vinduer i for eksempel kontrollrom monteres/lukkes og låses, ekstra kraftverksporter låses, bjelkestengsel legges på plass.
- Visuell avskjerming av vitale komponenter.
- Ekstra opplysning av områder eller lyskastere over området (observere og blende)[3].
- De kraftforsyningsanlegg som er prioritert for forsvarsmessig vakthold klargjøres for dette, se § 5-6 Vakthold.

5.5.3 Brannsikkerhet

Brann i eller nær driftskontrollsystemet må oppdages så fort som mulig, slik at slukkearbeidet kan starte tidligst mulig og konsekvensene begrenses. Enheter med driftssentraler i alle klasser må derfor installere automatisk brannalarmanlegg med detektorer i alle rom i den delen av bygget hvor driftssentralen med tilbehør er plassert. Dette er:

- Driftssentralen med tilhørende tekniske rom.
- Alle rom i samme branncelle (minimum EI 60 brannmotstand) som driftssentralen.
- Alle naborom i samme brannseksjon (minimum REI 120 M brannmotstand) som driftssentralen.
- Alle naborom i samme brannseksjon (minimum REI 120 M brannmotstand) som tilhørende tekniske rom.
- Alle rom som ligger over eller under driftssentralen og/eller tilhørende rom dersom etasjeskillene ikke tilfredsstiller REI 120 M brannmotstand, bygget er fullsprinklet, eller annet som gir tilsvarende sikring mot spredning av røyk og brann.

---

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

Brannalarmen skal døgnkontinuerlig varsle driftspersonell, enten stedlig personell eller hjemmevakt. Enheten må sørge for:

- Et tilstrekkelig antall detektorer, sammenkoblet i et system, med forskjellige egenskaper (ioniske, optiske og varmesensitive).
- Et system for å effektivt og hurtig motta og reagere på deteksjon.
- Nødvendig slukkeutstyr av hensiktsmessig type, antall og plassering.

Om mulig bør brannvarsling også gå til lokal brann- og redningsetat.

5.5.3.1 Driftssentraler, klasse 1

Driftssentral med tilbehør bør skilles av i egen branncelle som minst bør tilfredsstille brannmotstandsklasse EI 30 med EI 30 dører (selvlukking vurderes). Det forventes tilsvarende sikkerhetsnivå for kabelgjennomføringer med mer.

5.5.3.2 Driftssentraler, klasse 2

Driftssentral med tilbehør må skilles av i egen branncelle som minst må tilfredsstille brannmotstandsklasse EI 60 med EI 60 (C) dører (selvlukking vurderes). Det forventes tilsvarende sikkerhetsnivå for kabelgjennomføringer med mer.

5.5.3.3 Driftssentraler, klasse 3

Driftssentral med tilbehør må skilles av i egen branncelle som minst må tilfredsstille brannmotstandsklasse REI 60 i vegg/dekke minimum med EI 60 (C) dør (tidligere A 60 S) (selvlukking vurderes). Det forventes tilsvarende sikkerhetsnivå for kabelgjennomføringer med mer. Motstandstiden økes til 120 minutter dersom det ikke er installert automatisk slukkeutstyr. Ved dokumentert nærhet til permanent bemannet brannutrykningsenhet kan sistnevnte krav reduseres, men ikke til mindre enn REI 60, da dette også skal tjene som skallsikring.

5.5.4 Opprettholdelse av sikringstiltak ved vedlikehold, reparasjoner o.l.

Alle nødvendige sikringstiltak, for anlegg i alle klasser, bør være ferdig montert og sikret mot at de fjernes av uvedkommende. Bare ved arbeid på stedet, kan beskyttelsestiltak helt eller delvis fjernes av praktiske grunner og av hensyn til arbeidssikkerheten. I slike situasjoner forutsettes på forhånd grundige risikovurderinger og kompenserende tiltak. Om skallsikringen må svekkes under arbeidet, må det vurderes å styrke områdesikringen, og omvendt. Er det ikke mulig å oppnå tilstrekkelig sikringsnivå på denne måten, må vakthold vurderes. Anleggene skal være sikret når arbeidsstedet forlates for dagen.

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

Arbeid som medfører hulltaking i brannskiller eller fjerning av branntetting, må gis særlig oppmerksomhet. Permanent eller midlertidig branntetting må etableres før arbeidsstedet forlates for dagen.

Ved arbeid som går over flere dager må det være et godt system for kontroll med at alle typer sikringstiltak er funksjonelle når arbeidsstedet forlates.

Om adgangskontroll må deaktiveres eller endringer gjøres på sensorer, kabler, kameraer o.l. må en likeledes forsikre seg om at funksjonaliteten er gjenopprettet før annen sikring eller vakthold oppheves.

5.5.5 Oppdagelse av hendelser og handlinger

5.5.5.1 Kraftforsyningsanlegg i klasse 1

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

Systemer for oppdagelse/alarm ved eksempelvis innbrudd, brann og teknisk svikt anbefales. Der lokale risikoforhold tilsier det, forutsettes slike alarmsystemer iverksatt

5.5.5.2 Kraftforsyningsanlegg i klasse 2

For kraftforsyningsanlegg i klasse 2 skal det være tiltak som dokumenterer evne til raskt å oppdage og kunne håndtere uønskede hendelser og handlinger på en effektiv måte. I tillegg til regelmessig tilsyn og gode rutiner, må det minst være installert innbrudds- og brannalarm i alle viktige deler av anlegget som effektivt varsler vaktsentral, driftssentral eller annet relevant personale[4]. Tiltakene skal også vurderes for administrasjonsbygg, lager med videre av betydning for ledelse og drift, beredskap og sikkerhet. Det bør videre være ordninger for raskt å kunne sende ut folk for stedlig observasjon, verifikasjon og treffe de tiltak som situasjonen krever.

Det skal til enhver tid holdes kontroll på hvem som har rettmessig adgang til anlegget, i henhold til § 4-5 Adgangskontroll.

Det må i tillegg være gjennomførbare planer for skjerpet tilsyn og kontroll med anlegg i ekstraordinære situasjoner.

5.5.5.3 Kraftforsyningsanlegg i klasse 3

Alle kraftforsyningsanlegg i klasse 3 skal utstyres med mekanismer for straks å oppdage uønskede hendelser og handlinger.

Dette forutsetter ordninger som gjør det mulig å få umiddelbar varsel til kompetent personale om all uønsket ferdsel og handlinger innenfor et definert område som minst må omfatte anleggets vitale komponenter med eventuell tilhørende skallsikring. Det må i tillegg være varslingsordninger som gjør det mulig med umiddelbar oppfølging av hendelsen.

Dette innebærer som minimum innbrudds- og brannalarm til døgnbetjente sentraler som sikrer umiddelbar oppfølging av en uønsket situasjon. Innbrudds- og brannalarm må som minimum omfatte alle viktige deler (for anleggets forsyningsmessige funksjon) av anlegget.

Det bør i tillegg være kameraovervåkning eller tilsvarende. Dette for å sikre en raskest mulig oversikt over hva som kan ha skjedd. Systemet må ikke kunne omgås, narres eller settes ut av spill uten at dette oppdages.

---

[4] For brannvarslingssystemer henvises det også til DSBs veiledning til FEF § 4-9.

Ved valg av kameraovervåkningssystem er det viktig å passe på personvernhensyn, dialog med ansatte og overholdelse av Personopplysningsloven.

- Følge Datatilsynets regler for ”Fjernsynsovervåkning” - i henhold til Lov om behandling av personopplysninger (personopplysningsloven) og forskrift om behandling av personopplysninger (personopplysningsforskriften)
- Herunder skal det bl.a. ved skilt eller på annen måte varsles om at overvåkning finner sted.
- Det vises også til at det normalt kun er tillatt å oppbevare opptak i sju dager. Men det finnes relevante unntak - bl.a. ved sannsynlig politietterforskning.

Det forutsettes videre ordninger for rask utrykning av kompetent personale, og det bør vurderes bruk av for eksempel signaler (lys, lyd og liknende) på anlegget for å varsle uvedkommende.

Det må i tillegg være gjennomførbare planer for skjerpet overvåkning av anlegg i ekstraordinære situasjoner.

Se for øvrig veiledningens punkt 5.5.10 i forhold til praktisering på eksisterende anlegg.

5.5.6 Effektiv gjenoppretting

For generelle krav til gjenoppretting, se § 3-5 Gjenoppretting av funksjon. I tillegg har anlegg i klasse 2 og 3 særlige krav til gjenoppretting etter denne paragrafen. Siden dette omfatter tunge komponenter med mulig lange leveringstider, er det viktig at gjenoppretting planlegges nøye med hensyn til hvordan ulike komponenter kan erstattes og midlertidige improvisasjoner kan utføres.

Selv om havari/utfall av en viktig komponent eller anleggsdel ikke nødvendigvis fører til strømutfall eller andre umiddelbare konsekvenser av vesentlig betydning, svekker dette redundansen og fleksibiliteten i systemet. Dette kan få alvorlige følger om nye feil eller ekstraordinære situasjoner inntreffer. Sikringstiltak skal derfor ikke bare foretas ut fra partielle vurderinger av enkeltfeil, men ut fra systemmessige vurderinger av flere samtidige hendelser. Av samme grunn må gjenoppretting av betydelige havarier starte uten ugrunnet opphold.

Denne bestemmelsen pålegger ingen å gjennomføre risikofylte oppdrag med fare for eget liv og helse. Ved indikasjoner (gjennom verifikasjon av hendelsen) på at en slik situasjon er under utvikling, skal det ventes på tilstrekkelige forsterkninger, eventuelt vedkommende nødetat. Det forutsettes at ansvarlige personer og personell på stedet utviser et lokalt skjønn.

5.5.7 Redundans i anlegg og system

Med redundans menes her at et kraftforsyningsanlegg anordnes og utrustes slik at en enkelt feil eller hendelse ikke slår ut anleggets vitale funksjoner i det kraftsystemet det er en del av. Det vil si at det finnes andre komponenter eller deler av anlegget som automatisk eller ved rask manuell omkobling eller annen inngripen kan overta funksjon til feilbefengt eller ødelagt anleggsdel. En metode for å oppnå slik redundans, er dublering (jf. alternativer) av viktige komponenter – gjerne i kombinasjon med fysisk og elektrisk atskillelse ved avstand eller fysisk beskyttelse. Eksempel vil være (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 (f.eks. ved brann) samtidig blir da svært liten.

Alternativt kan redundans anordnes ved at et annet anlegg kan overta det vesentlige av funksjonen til et havarert anlegg – for eksempel at det finnes to alternative innføringsstasjoner i et forsyningsområde. Merk at dette er lokal analogi til, men ikke helt det samme som et mer overordnet N-1 systemkrav til ordinær driftssikkerhet.

Manglende redundans kan i noen grad kompenseres ved evne til rask gjenoppretting ved f.eks. planlagt og fysisk forberedt forbi-/omkobling.

5.5.7.1 Høyspentanlegg

Klasse 1, 2 og kraftstasjoner klasse 3 – her vurderes dublering av høyspentkomponenter i hvert enkelt tilfelle.

Klasse 3 - nettanlegg (transformatorstasjoner og koblingsanlegg for kraftstasjoner) bør som hovedregel ha dublering av de viktigste komponentene for anleggets funksjoner. Dette gjelder bl.a. hovedtransformatorer, samleskinner, effekt og skillebrytere.

5.5.7.2 Hjelpesystemer

For driftskontrollsystem, se § 6-4 Særlige krav til driftskontrollsystem.

For øvrige anlegg vurderes behovet for dubleringer og liknende av kontrollsystemet inne i det enkelte anlegg i hvert enkelt tilfelle.

For klasse 3 alle anlegg - legges både viktige hhv. strøm og styrekabler i hver sine egne fysisk separate traseer.

For strømforsyning og nødstrømsanlegg, se punkt 5.5.8 i denne paragrafen.

Anlegg i klasse 2 og 3 utstyres med effektive vern og overspenningsavledere. Når det gjelder tiltak for å forhindre teknisk svikt og annen skade, vises det til:

- Energilovforskriften (FOR-1990-12-07-959) § 3-4. Vilkår for konsesjon på elektriske anlegg, drift og vedlikehold mv.
- Forskrift om systemansvaret i kraftsystemet (FoS) – (FOR-2002-05-07-448) med veiledning utgitt av Statnett.
- Forskrift om elektriske forsyningsanlegg (FOR-2005-12-20-1626) med veiledning fastsatt av DSB.
- Forskrift om kvalifikasjoner for elektrofagfolk (FOR-1993-12-14-1133).

5.5.8 Anleggenes egen strømforsyning, nødstrøm

5.5.8.1 Generelt

For alle klassifiserte anlegg – særlig anlegg i klasse 2 og 3, samt alle driftskontrollanlegg, må anleggenes egen strømforsyning (inkludert nødstrøm) gis stor oppmerksomhet, og utføres med tilstrekkelig robusthet og utholdenhet, slik at de virker til enhver tid. Det forytsettes at veiledningen til FEF kapittel 4 Høyspenningsinstallasjoner, følges.

Ved vurdering av behovet for nødstrøm må det blant annet tas hensyn til følgende forhold:

- Hele driftskontrollsystemets betydning og klasse, også kontrollfunksjonene ute i det enkelte anlegg
- Det enkelte anlegg, den enkelte komponent og sambandsvei sin betydning for driftskontrollfunksjonene
- Vedkommende anleggs tilknytning til det lokale/regionale strømnettet og kvaliteten på dette
- Anleggenes utstyr, interne forhold og egenforbrukets art (maksimal last, forbruk i feilsituasjoner, motorlast/ vekselretter og liknende)
- Geografiske, topografiske og værmessige forhold (avsides eller sentral beliggenhet)
- Betjeningsforhold og tilgjengelighet med hensyn til veiforbindelse med mer
- Logistikk med hensyn til fremføring og etterfylling av diesel til faste og mobile nødstrømsaggregater må beregnes og planlegges, også når forholdene gjør tilgjengelighet vanskelig

Ved alle anlegg må det foretas en gjennomgående systemtenkning og totalvurdering (ROS) av strømforsyningen, se § 5-4 Analyse.

5.5.8.2 Drift og gjenopprettingsevne, kontroll og vedlikehold

For anlegg i alle klasser gjelder at anleggenes egne strømanlegg med nødstrømsforsyning skal plasseres og konstrueres slik at risikoen for skade og uhell blir minst mulig. De må kunne tåle de maksimalbelastningene de kan bli utsatt for, herunder kunne forsyne nødvendige hjelpesystemer som for eksempel nødlys og kjøling. Normalt bør det legges opp prioriterte kurser for de viktigste funksjonene som styrestrøm, kontrollrom og belysning i viktige deler av anlegget.

Anleggenes egne strømanlegg med nødstrømsforsyning skal til enhver tid holdes i forsvarlig og driftsklar stand. Ved regelmessige mellomrom skal de testes både med hensyn til funksjon og kapasitet/yteevne og utholdenhet. Minst en gang i året bør nødstrømsanleggene testes med prioritert last og ved at ordinær strømforsyning kobles fra.

Det vises for øvrig til §§ 3-4 Drift og 3-5 Gjenoppretting av funksjon.

Nærmere veiledning til utførelse av strømforsyning og nødstrøm ved de enkelte typer anlegg etter klasse er gitt i vedlegg 1 til denne veiledningen. Dette vedlegget er underlagt taushetsplikt etter beredskapsforskriften § 6-2 og unntatt fra innsyn etter offentleglova § 13, 1. ledd.

5.5.9 Kompetent bemanning av anlegg

5.5.9.1 Generelt

Det er en grunnleggende forutsetning at KBO-enheten skal kunne drifte sine anlegg med kompetent betjening.

Hensiktsmessigheten av å bemanne anlegg ordinært eller ekstraordinært må vurderes lokalt i hvert enkelt tilfelle. Dette nedfelles i enhetens beredskapsplan.

Bestemmelsene i denne paragrafen stiller krav til at bemanning av anlegg skal være mulig ved hjelp av planer og tilgjengelige kapasiteter (antall, opplæring, øvrige ressurser og øvelser). Eksempler på situasjoner som kan kreve ekstraordinær bemanning:

- Feil/skader og driftsforstyrrelser i anlegg/system.
- Bortfall av automatiske driftskontrollfunksjoner, anlegg må styres lokalt.
- Beredskapssituasjoner som krever særlig vakthold/årvåkenhet og beredskapsmessige forberedelser.
- Etter vedtak (for eksempel erklært beredskap) fra sentral myndighet.

Med kompetanse menes både nødvendig kunnskap om anlegget, hvordan det lokalstyres og formell kompetanse i forhold til selvstendig adgang til høyspentanlegg, se forskrift om sikkerhet ved arbeid i og drift av elektriske anlegg.

Det er ikke stilt noen eksplisitte krav til utholdenhet, men om det oppstår en situasjon som krever ekstraordinær bemanning av anlegg, er det påregnelig at denne kan vare en stund til mer normal drift er gjenopprettet eller situasjonen forøvrig har normalisert seg. Det bør planlegges for minst to døgn med et opplegg for logistikk og avløsning, som eventuelt kan forlenges. Hensynet til regler for arbeidstid og liknende forutsettes ivaretatt.

I det etterfølgende gis i tillegg en mer spesifikk veiledning i forhold til klasse.

5.5.9.2 Kraftforsyningsanlegg i klasse 1

Ingen spesielle krav utover de generelle kravene ovenfor.

5.5.9.3 Kraftforsyningsanlegg i klasse 2

§ 5-5 b 3. ledd:

Anlegget skal kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriftens § 3-4.

Tiltaket planlegges av vedkommende enhet i KBO, som må ha nødvendige kapasiteter, antall, opplæring, øvrige ressurser og øvelser for dette.

5.5.9.4 Kraftforsyningsanlegg i klasse 3

§ 5-5 c 3. ledd:

Alle anlegg skal samtidig og innen rimelig tid kunne betjenes lokalt av kompetent bemanning i ekstraordinære situasjoner etter krav i denne forskriftens § 3-4.

Krav som i ovennevnte. I tillegg skal alle anlegg i klasse 3 kunne bemannes samtidig innen rimelig tid.

Ved begrepet ”innen rimelig tid” er det her tatt hensyn til at det mange steder kan være store avstander, og at relevant personell i utgangspunktet kan være opptatt andre steder med andre viktige gjøremål, eller må innkalles. Berørte anlegg bør likevel kunne bemannes i løpet av få timer. I forhold til meget omfattende situasjoner bør selskapet ha vurdert dette i sine risikovurderinger og ha en gjennomtenkt beredskap/prioritering.

5.5.10 Praktisering av bestemmelsene for eksisterende anlegg

Etter energiloven kapittel 9 Beredskap kan det kreves gjennomført nye eller endrede tiltak ved både nye og eksisterende kraftforsyningsanlegg. I det etterfølgende gis for disse en særlig veiledning i hvordan forskriftens bestemmelser normalt vil bli praktisert i forhold til eksisterende anlegg, og en indikasjon på hvordan NVE vil følge dette opp under tilsyn. Fremstillingen er forenklet og antyder minimumsløsninger. Vi understreker at det uansett er den enkelte enhet som selv har ansvaret for å vurdere og iverksette tilstrekkelige sikringstiltak ved sine anlegg. Det må også understrekes at det her er tatt hensyn til de mange eldre kraftforsyningsanlegg, og at dette punkt ikke gir noe generell dispensasjon verken fra beredskapsforskriftens bestemmelser eller fritak fra tidligere pålegg som ikke er gjennomført.

5.5.10.1 Eksisterende kraftforsyningsanlegg som skal bygges om eller utvides

Her følges øvrige relevante punkter i denne veiledningen for den del av anlegget som skal bygges om eller utvides med de tilpasninger som må gjøres både på ny og gammel del av anlegget for at det skal bli et helhetlig og balansert sikringsnivå. For øvrige deler av anlegget gjelder nedenstående.

5.5.10.2 Eksisterende kraftforsyningsanlegg forøvrig

Som hovedregel kreves det ikke utført sikringstiltak som medfører større ombygginger av eksisterende anlegg. Unntak kan gjøres for særlig viktige eller særlig dårlig sikrede anlegg. Dette innebærer at det normalt ikke kreves iverksatt tiltak som innebærer vesentlige endringer i så som planløsninger, bygningsmasse eller i arrangeringen av de elektriske høyspenningsanlegg.

Dersom det er vedtatt eller det foreligger konkrete planer for at anlegget likevel skal ombygges eller utvides i relativt nær fremtid (< 10 år), kan det vurderes om relevante sikringstiltak for de delene som skal bygges om, inntil videre utstår og heller medtas i denne ombyggingen. Dette gjelder bare for relativt kostbare tiltak eller når lapping på et eldre anlegg ikke synes hensiktsmessig. Nevnte vurdering og planer må i så fall kunne dokumenteres og annen kompenserende beredskap forberedes.

For de bestemmelsene hvor anleggets art og alder ikke har vesentlig betydning for gjennomføringen av tiltaket, gjelder denne veiledningen som for nye anlegg. Dette omfatter analyser, beredskapsplaner, adgangskontroll, reparasjonsberedskap, betjening av kompetent bemanning, kontroll og vedlikehold.

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

5.5.10.3 Oppdagelse og reaksjon

Klasse 1

Det er normalt tilstrekkelig med et regelmessig tilsyn og rutiner for å håndtere hendelser og unormale tilstander. Ved utsatte anlegg bør alarmer vurderes som for klasse 2.

Klasse 2

I tillegg til ovennevnte for klasse 1 må det minst installeres innbrudds- og brannalarm i viktige deler av anlegget som effektivt varsler vaktsentral, driftssentral eller annen betjening.

Det skal til enhver tid holdes kontroll på hvem som har adgang til anlegget.

Klasse 3

I tillegg til ovennevnte for klasse 1 og 2 bør det også installeres kameraovervåkning som kan gi tilstrekkelig oversikt over uønskede hendelser når anlegget ikke er bemannet. For å vinne erfaring forventes det at alle eiere av anlegg i klasse 3 har minst et anlegg med system for oppdagelse av uønskede hendelser. NVE vil komme tilbake til denne saken med nærmere enkeltvedtak og veiledning etter hvert som mer erfaring vinnes.

5.5.10.4 Områdesikring alle klasser

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

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

5.5.10.5 Skallsikring

Klasse 1

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

Klasse 2

I tillegg til ovennevnte for klasse 1

a. Alle dører o.l. som er eller bør være en del av de fysiske sikringstiltak etter BfK - utvendig eller innvendig – må minst fylle kravene til ståldør A 60 etter tidligere standard. Tilsvarende må alle vinduer som er eller bør være en del av skallsikringen rundt vitale deler av anlegget, som et minimum være utført som hærverkshemmende ved glass, gitter eller liknende. Øvrige mulige atkomster (kabelsjakter, luftekanaler o.l.) sikres tilsvarende. Der nye tiltak må utføres for å fylle disse kravene, søkes så langt mulig disse utført etter punkt 5.5.2 i denne veiledningen. For f.eks. eldre kraftstasjoner i dag som i sin tid ble utført med mange eller store vindusflater, kan det gjøres unntak, men kompenserende tiltak som alarmer eller liknende må da vurderes.

b. Hovedtransformatorer i klasse 2 anlegg bør skallsikres. Der dette ikke er gjort i det hele tatt, må dette utføres etter punkt 5.5.2 i denne veiledningen ved neste ombygging eller utvidelse av anlegget. Der dette delvis er utført, må tiltaket fullføres ved at for eksempel transport-, inspeksjons- og lufteåpninger så langt mulig sikres med porter, gitter etter punkt 5.5.2 i denne veiledningen. I anlegg med god redundans kan det aksepteres at f.eks. bare en av to transformatorer sikres.

c. Kraftstasjoner i klasse 2 i fjell sikres med minst en solid og låsbar port, gitter eller liknende i alle atkomster som fører inn til stasjonens vitale deler. Der nye tiltak må utføres for å fylle disse kravene, søkes så langt mulig disse utført etter punkt 5.5.2 i denne veiledningen.

Klasse 3

I tillegg til ovennevnte for klasse 1 og 2

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

a. For å oppfylle BfKs krav må som hovedregel alle krafttransformatorer i klasse 3 kraft-forsyningsanlegg skallsikres, så langt praktisk mulig. Der skallsikring og ulike former for beskyttelse i noen grad er utført, kan det bygges videre på dette. Transport-, inspeksjons- og lufteåpninger må så langt mulig sikres med porter, gitter etter punkt 5.5.2 i denne veiledningen.

b. For å oppfylle BfKs krav må som hovedregel alle kraftstasjoner i klasse 3 (i fjell) i tillegg til dagport, sikres med minst en solid og låsbar stålport, gitter eller liknende i alle atkomster (kabelsjakter, luftekanaler o.l.) som fører inn til stasjonens vitale deler (herunder også lukehus o.l.). Der nye tiltak må utføres for å fylle disse kravene, søkes så langt mulig disse utført etter 5.5.2 i denne veiledningen.

5.5.10.6 Låseanordninger – alle klasser

For å oppfylle BfKs krav må alle låser med beslag og innfesting på stengsler som inngår i område- og skallsikring være FG-godkjent eller tilsvarende. I områdesikringen bør det minst brukes FG klasse 2 og for skallsikring FG klasse 3. Hvis låsene for å oppfylle dette kravet likevel må skiftes ut, brukes FG/ sikkerhetsklasse for vedkommende anlegg og klasse som i punkt 5.5.2 i denne veiledningen.

5.5.10.7 Hjelpesystemer (strøm og IKT)

Alle klasser

De funksjonelle kravene BfK stiller til kraftforsyningsanleggenes egen strømforsyning inkludert nødstrøm, og til driftskontroll/ anleggenes styresystemer, er av stor viktighet. Som hovedregel bør derfor 5.5.7 og 5.5.8 i denne veiledningen oppfylles for vedkommende anlegg og klasse, med nødvendige tillempninger etter anleggets art og utforming. Alle anlegg må gjennomgås regelmessig og nødvendige utbedringer foretas.

Klasse 2 og 3

For klasse 2 og 3 er hovedkravet at en enkelt feil eller hendelse ikke kan sette funksjonen, og dermed kraftforsyningsanlegget eller noen av dets vitale komponenter ut av spill. På dette punktet må anleggene gjennomgås og åpenbare svakheter rettes. Batteribank med tilstrekkelig kapasitet må være installert og nødstrømsaggregat må kunne kobles til.

Klasse 3

For klasse 3 anlegg må minst både viktige hhv. strøm og styrekabler legges i hver sine egne fysisk separate traseer. Batteribankene må oppgraderes til å holde de tider som nevnt i punkt 5.5.8 i denne veiledningen og bør dubleres i separate rom. Nødstrømsaggregat må være installert eller tilgjengelig på kort varsel.

5.5.10.8 Redundans

Klasse 2 og 3

Med unntak av ovennevnte hjelpesystemer kreves det normalt ikke ombygging eller anskaffelse av tyngre komponenter for å oppnå redundans. Manglende redundans må i så fall søkes kompensert ved bl.a. beredskapsplaner og reparasjonsberedskap. F.eks. må det finnes en konkret plan for hvordan hovedtransformatoren erstattes av en annen. Ved manglende redundans (brytere, samleskinne ol) i koblingsanlegget må det finnes planer, utstyr, reservedeler og kompetanse for rask forbikobling til ordinær gjenoppretting har funnet sted.

§5-6 Vakthold

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

Eier skal herunder bidra til å:

a) Påvise anleggets vitale deler og beskaffenhet forøvrig,

b) anskaffe materiell og gjennomføre øvrige sikringstiltak for å hjelpe vaktstyrken, og

c) tilrettelegge for øvelser på anleggets område, herunder inngjerdet høyspenningsområde og liknende.

Veiledning

Ved ekstraordinære situasjoner som fører til økt beredskap, kan det bli nødvendig å etablere ekstra vakthold ved en del kraftforsyningsanlegg som av NVE og andre myndigheter er vurdert som særlig viktige.

Kriterier for utvelgelse beskrives ikke i denne veiledningen, men aktuelle enheter i KBO er informert om dette. Ved behov kan NVE gi nærmere informasjon.

5.6.1 Planlegging og gjennomføring

Denne bestemmelsen pålegger eier av vedkommende prioriterte kraftforsyningsanlegg/objekt en del plikter.

5.6.1.1 Påvise anleggets vitale deler og beskaffenhet forøvrig

Enheten må legge følgende faktorer til grunn:

- Momentane konsekvenser av skade/ødeleggelse.
- De ulike anleggenes sårbarhet og beskyttelse.
- Reparasjonsmuligheter og erstatningstider.
- Alternativer, muligheter for omlegginger og improvisasjoner.

5.6.1.2 Anskaffe materiell og gjennomføre øvrige sikringstiltak for å bistå vaktstyrke

Informasjon finnes i direktiv: Objektsikring - vakthold og sikring av kraftforsyningsanlegg, NVE, januar 1995. Dette direktivet er gradert BEGRENSET etter sikkerhetsloven og utleveres bare til personer som er autorisert for denne graderingen og har tjenstlig behov.

5.6.2 Øvelser ved høyspenningsanlegg

NVE har i samarbeid med Elektrisitetstilsynet (nå Direktoratet for samfunnssikkerhet og beredskap) fastsatt et eget øvingsdirektiv: Direktiv for øvelser ved m.m. ved kraftforsyningsanlegg på www.nve.no. Dette gir de ulike parter ved slike øvelser klare plikter og rettigheter og skal følges ved alle øvelser i forbindelse med høyspenningsanlegg.

§5-7 Kontroll og vedlikehold

Eier av anlegg skal føre kontroll med at pålagt og gjennomførte sikringstiltak så som utstyr, materiell, fysiske og elektroniske anordninger er tilstede, fungerer etter hensikten og at nødvendig vedlikehold utføres.

Veiledning

Med sikringstiltak forstås her tiltak iht. bestemmelsene i beredskapsforskriften.

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

Enheten må sørge for at følgende blir gjennomført og dokumentert:

- Identifisere hvilke sikringstiltak som er pålagt og gjennomført for anlegget.
- Lage en oversikt over sikringstiltakene, både aktive og passive.
- Lage en beredskapsplan for bruken av tiltakene, når tiltakene skal settes i verk, hvem som skal gjøre hva og hvilke ressurser det er behov for (verktøy, maskiner, med mer).
- Innarbeide kontroll og vedlikehold av sikringstiltakene i enhetens vedlikeholdssystem/kvalitetssystem, som sikrer en fornuftig frekvens på kontrollene.
- Funksjonsteste sikringstiltakene jevnlig, for å se om de fungerer etter hensikten. Dette er spesielt viktig for de passive sikringstiltakene.

- Sørge for at defekte tiltak erstattes eller repareres.
- Andre nødvendige tiltak for at sikringstiltakene fungerer hensiktsmessig.

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

Kap 6 Informasjonssikkerhet

Bestemmelsene om informasjonssikkerhet gjelder for all informasjon, enten den befinner seg elektronisk, på papir eller uttales muntlig.

§ 6-4 Særlige krav til driftskontrollsystemer er en paragraf som spesialregulerer området driftskontrollsystemer, og kommer i tillegg til IT-sikkerhetskravene i andre deler av beredskapsforskriften. Bestemmelsen gjelder derimot ikke for andre IT-systemer.

I dette kapitlet omfatter IT-sikkerhet også samband og annen elektronisk kommunikasjon, se § 3-8 Samband. Det vil si at begrepet IT brukes synonymt med IKT-begrepet.

KBO-enhetene bør utvikle en egen sikkerhetspolicy med tilhørende retningslinjer.

§6-1 Generelt

Alle enheter i KBO skal foreta en løpende helhetlig vurdering av informasjonssikkerheten. Nødvendige tiltak og rutiner skal etableres og vedlikeholdes.

Informasjonssikkerheten i kraftforsyningen skal omfatte konfidensialitet, integritet og tilgjengelighet av informasjon og ressurs. Dette skal gjelde følgende områder:

a) Sensitiv informasjon om kraftforsyningen som kan brukes til å hindre eller skade kraftforsyningens funksjoner,

b) alle systemer og enheter som ivaretar viktige driftskontrollfunksjoner – herunder både informasjonsbehandling og kommunikasjon - for henholdsvis: driftssikkerhet, overvåking, styring, vedlikehold og feilretting av kraftsystem, anlegg, og vassdragsregulering for kraftproduksjon,

c) administrative og merkantile systemer som behandler sensitiv informasjon, eller har betydning for driften av kraftforsyningen.

Alle enheter i KBO skal utpeke en egen datakyndig IT-sikkerhetsleder. Denne skal bistå enhetens leder med informasjonssikkerheten. IT-anlegg skal plasseres slik at mulighetene for skade blir minst mulig.

Veiledning

6.1.1 Løpende, helhetlig vurdering

Enheten må gjennomføre en løpende helhetlig vurdering av egen håndtering av informasjon og bruk av IKT-systemer. Hensikten med dette er å gjøre enheten i stand til å oppdage og håndtere brudd på og trusler mot informasjonssikkerhet raskt, samt identifisere og redusere risiko og sårbarhet. Enheten må derfor ha dokumenterte rutiner som sikrer at informasjonssikkerheten er ivaretatt, eksempelvis:

- Oppdaterte ROS-analyser og instrukser
- Opplæring i informasjonshåndtering
- Gjennomføre logginger og jevnlige vurderinger
- Ha et system for å rapportere hendelser knyttet til informasjonssikkerheten og brudd på denne til overordnede ledd i egen organisasjon, samt oppfølging av slike hendelser i organisasjonen

Eksempler på informasjonssikkerhetsforhold som bør vurderes i ROS-analyser:

- Avhengigheten til IKT-systemer, som internett, eksterne og interne IKT-systemer, GPS og mobiltelefoni, leverandører og eksterne tjenesteleveranser.
- Sårbarhet ved bruk av trådløse datanett, IP-telefoni (VoIP), eller bærbare enheter (laptop, minnepinne, mobiltelefoner).
- Tillegg og endringer i informasjonssystemer eller aksessmuligheter.
- Innbrudd i anlegg eller IKT-system.
- Angrep av ondsinnet programvare.
- Hendelige uhell og operatørfeil.
- Sensitiv informasjon på avveie.
- Tekniske feil.

Enheten må gjennomføre løpende og helhetlig vurdering av informasjonssikkerheten for alle anlegg og systemer.

Prinsippene for informasjonssikkerhet gjelder for alle informasjonsbærere. Blant annet:

- Elektronisk
- På papir
- Ansattes kunnskap

6.1.2 Konfidensialitet, integritet og tilgjengelighet

Med konfidensialitet menes at sensitiv informasjon kun skal være tilgjengelig for rettmessig bruker, utstyr eller prosess.

Med integritet menes at informasjonen skal være korrekt, relevant og pålitelig, og ikke kan manipuleres.

Med tilgjengelighet menes at informasjon og ressurs er tilgjengelig og anvendelig til enhver tid.

6.1.3 Typer informasjon som anses som sensitiv

Bokstav a gir en generell definisjon av sensitiv informasjon. Bestemmelsen må leses i sammenheng med § 6-2 Beskyttelse av informasjon, som gir detaljert regulering av hva som er sensitiv informasjon. Enheten må utover dette selv gjøre en vurdering av om den har ytterligere informasjon som kan brukes til å hindre eller skade kraftforsyningens funksjoner.

6.1.4 Ivaretakelse av driftskontrollfunksjoner

Bokstav b gir en definisjon av hva som menes med driftskontrollfunksjoner og IKT-systemene som ivaretar disse. Bestemmelsene om konfidensialitet, integritet og tilgjengelighet gjelder for ovennevnte funksjoner og systemer.

6.1.5 Administrative og merkantile systemer

Bestemmelsens annet ledd, bokstav c omfatter administrative og merkantile systemer som har betydning for drift og sikkerhet og/eller inneholder sensitiv informasjon.

6.1.6 IT-sikkerhetsleder

IT-sikkerhetsleder har viktige oppgaver innenfor oppfølging av IT-sikkerhet, spesielt for driftskontrollsystemet, men også for andre systemer som inneholder informasjon som er viktig for driften, eller som må avskjermes for uvedkommende. IT-sikkerhetsleder bør:

- Planlegge og følge opp IT-sikkerheten
- Bidra til å identifisere og skjerme sensitiv informasjon om kraftforsyningen og håndtere viktig informasjon
- Være NVEs kontaktperson på IT-sikkerhetsspørsmål

For kompetansekrav til IT-sikkerhetsleder, se § 3-2 Kompetanse.

Det er viktig at IT-sikkerhetsleder integreres godt med øvrig relevant sikkerhets- og beredskapsarbeid i enheten.

Enhetens leder har det overordnede ansvar for informasjonssikkerheten etter § 4-1 Ansvar og organisering. IT-sikkerhetsleder bør kunne rapportere direkte til daglig leder ved behov.

6.1.7 Plassering av IT-anlegg

Enheten må gjennomføre ROS-analyser etter §§ 5-4 Analyse og 1-3 Risiko- og sårbarhetsanalyse for å utforme og plassere IT-anlegg, slik at mulighetene for skade blir minst mulig. Det skal fremgå hvor anlegget best kan plasseres blant annet fysisk, elektronisk og logisk for å unngå skader som følge av teknisk svikt, naturgitt skade og påført skade.

6.1.8 Henvisninger

Norsk senter for informasjonssikring (NorSIS) sin veiledning ”Sikkerhetsledelse” beskriver viktige arbeidsoppgaver for en sikkerhetsleder, se www.norsis.no

Ved vurdering av trusselbildet kan bakgrunnsinformasjon hentes fra blant annet:

NorSIS, www.norsis.no

NSMs årlige risikovurdering: www.nsm.stat.no

Veiledning fra NorSIS, ”Håndbok for informasjonssikkerhet” (egnet for små og mellomstore virksomheter)

NSMs temahefte 1/2006 ”Sårbarheter og trusler mot informasjonssystemer”.

International Organization for Standardization ISO/IEC 27001 — Information security management systems — Requirements

ISO/IEC 27002 — Code of practice for information security management

Standard of Good Practice fra Information Security Forum (ISF), se www.securityforum.org

COBIT fra ISACA, se www.isaca.org

§6-2 Beskyttelse av informasjon

Sensitiv informasjon om kraftforsyningen skal ikke offentliggjøres.

På følgende områder skal sensitiv informasjon til enhver tid avskjermes effektivt for uvedkommende:

a) driftskontrollsystemer (oversikter over system, sikkerhetstiltak, sårbarhet og liknende)

b) detaljerte oversikter (kraftsystem, kart, tabeller og liknende) over sentral- og regionalnett hvor status over transformatorytelser eller kraftlinjer med spenningsnivå og/eller overføringskapasitet er angitt,

c) oversikter over fordelingsnett som leverer kraft til viktige forsvarsanlegg og andre beredskaps- og samfunnsviktige virksomheter,

d) sikrings- og sikkerhetstiltak,

e) beredskapsrom/kommandoplasser,

f) detaljerte analyser av sårbarhet som følge av påført skade,

g) oversikter over reservemateriellagre og reparasjonsmuligheter.

Herunder skal det vurderes hvilken informasjon som er viktig eller sensitiv for drift og sikkerhet. Det skal identifiseres hvor sensitiv informasjon befinner seg og hvem som er rettmessige brukere av denne informasjonen.

For denne informasjonen skal det etableres en effektiv tilgangskontroll, slik at kun rettmessige brukere har tilgang til informasjon og ressurser. Kommunikasjon skal beskyttes mot avlytting og manipulering av uvedkommende. Det skal utarbeides og implementeres sikkerhetsinstruks og gjennomføres tiltak og rutiner for å ivareta ovennevnte.

Norges vassdrags- og energidirektorat kan treffe vedtak om at informasjon om kraftforsyningen skal sikkerhetsgraderes og behandles i henhold til bestemmelsene i sikkerhetsloven.

Veiledning

Sensitiv informasjon om kraftforsyningen er informasjon som uvedkommende kan benytte for å skade eller hindre kraftforsyningen. Denne bestemmelsen bygger på § 6-1 og regulerer i detalj hva som er sensitiv informasjon om kraftforsyningen. Det vil likevel være tilfeller hvor også annen informasjon enn det som er omtalt i bestemmelsens annet ledd, vil kunne hindre eller skade kraftforsyningens funksjoner, se § 6-1 annet ledd bokstav a. Eksempelvis kan store mengder systematisert alminnelig informasjon om kraftforsyningen være kraftsensitiv informasjon om det i sum faller inn under noen av de ovennevnte punktene i forskriftsteksten. Bestemmelsen må leses i sammenheng med § 6-1 som blant annet gir en generell definisjon av kraftsensitiv informasjon.

For mer om sensitiv informasjon om vassdragsanlegg og deres funksjoner, se forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften, FOR-2009-12-18-1600) § 7-8.

6.2.1 Offentliggjøring og avskjerming

Sensitiv informasjon om kraftforsyningen er underlagt taushetsplikt, og enheten skal ikke gjøre slik informasjon offentlig tilgjengelig (legges ut på internett og liknende). Slik informasjon skal unntas fra innsyn etter lov om rett til innsyn i dokument i offentleg verksemd (offentleglova, LOV-2006-05-19-16). Det er den enkelte enhet sin plikt å vurdere hva som er sensitivt og sørge for avskjerming. Sensitiv informasjon merkes på følgende måte:

Taushetsplikt etter BfK § 6-2	**Teieplikt etter BfK § 6-2**
Unntatt offentlighet etter offl. § 13 første ledd	Unnateke offentleg innsyn etter offl. § 13 første ledd

Dersom et dokument er merket med taushetsplikt etter denne paragrafen, indikerer det at det er sensitiv informasjon i dokumentet. Enheten kan offentliggjøre de delene av dokumentet som ikke inneholder sensitiv informasjon.

6.2.2 Sensitiv informasjon som skal avskjermes

6.2.2.1 Driftskontrollsystemer

Informasjon om styresystemene knyttet til fysiske kraftforsyningsanlegg. Enheten skal ikke offentliggjøre følgende:

Samband:

- Beskrivelser, oversikter og illustrasjoner over kraftforsyningens stamnett for kommunikasjon.
- Beskrivelser, oversikter og illustrasjoner over viktige knutepunkter for elektronisk kommunikasjon.
- Beskrivelser, oversikter og illustrasjoner over beredskapssamband
- Sambandsplaner.

Driftssentraler:

- Systemskisser over styringssystemer med tilhørende brannmurer, samt eventuelle koblinger til administrative nett og internett.
- Omtale av hvilke kraftforsyningsanlegg som overvåkes eller styres fra en driftssentral, for eksempel i form av større nettbilder og koblingsmuligheter.
- Vaktordninger, bemanning og liknende.
- Svakheter og sårbare punkter, for eksempel nødstrøm og kjøling.
- Andre måter/steder å utøve driftssentralfunksjonen.

- Sikkerhetsprosedyrer og sikringstiltak ved driftssentralen med tilhørende driftskontrollsystem.

Det anbefales at det utvises forsiktighet med opplysninger om hvor driftssentralen er lokalisert.

6.2.2.2 Detaljerte oversikter

Dette kravet gjelder for systematiserte oversikter over sentral- og regionalnett, mellom 132 – 420 kV og liknende, med opplysninger om fysiske og elektriske egenskaper i form av:

- Transformatorytelser.
- Spenningsnivå.
- Overføringskapasiteter eller tverrsnitt.

Som detaljerte oversikter regnes blant annet:

- Kart over større områder med sentral- og regionalnettet inntegnet med spenningsnivå.
- Tabeller som lister opp større deler av sentral- og regionalnettet.
- Detaljerte beskrivelser av innføringsstasjoner til byer som viser helheten i systemet.
- Enlinjeskjemaer (for alle spenningsnivåer).
- Kart over jordkabelnettet.
- Bygningstegninger.

Erfaringsmessig må enhetene være særlig oppmerksomme for å unngå å offentliggjøre sensitiv informasjon om kraftforsyningen i følgende type dokumenter:

- Kraftsystemutredninger
- Lokale energiutredninger
- Konsesjonssøknader og meldinger i tilknytning til disse
- Profilering av selskapet på nettsidene

Dersom kraftsystemutredningen inneholder sensitiv informasjon, skal enheten i tillegg lage en egen offentlig utgave uten sensitiv informasjon om kraftforsyningen.

Konsesjonssøknader og meldinger i tilknytning til disse utgjør en egen utfordring med hensyn til å ikke offentliggjøre sensitiv informasjon om eksisterende kraftforsyningsanlegg. Sensitiv informasjon bør, etter avklaring med beredskapskoordinator, sendes i vedlegg. Legg merke til at bestemmelsen om beskyttelse av informasjon gjelder for planlagte og eksisterende anlegg, men ikke underveis i den løpende konsesjonsprosessen før konsesjon er gitt. Når endelig konsesjon er gitt skal sensitiv informasjon om det fjernes fra offentlig tilgang. For mer om konsesjonssøknader, se veileder for utforming av søknad om anleggskonsesjon for kraftoverføringsanlegg 10-06-2010.

6.2.2.3 Oversikter over fordelingsnett

Oversikter over fordelingsnettet omfatter detaljer om strømforsyningen til viktige bygninger eller anlegg for samfunnets ledelse og sikkerhet (som politi og offentlige myndigheter), forsvarsanlegg, kritisk infrastruktur, kommunikasjon, forsyninger, finans, viktig industri og liknende.

Opplysninger om fordelingsnett med tilhørende trafostasjon, innmating og nettstasjoner til slike objekter, er sensitiv informasjon. Bestemmelsen gjelder også enlinjeskjema og opplysninger om kabelnettet. Med fordelingsnett (distribusjonsnett) menes her hele forsyningskjeden fra transformator på overliggende nettnivå, og til og med siste forsyningsledd fram til sluttbruker.

6.2.2.4 Sikrings- og sikkerhetstiltak

Dette omfatter tiltak i forbindelse med bygningsmessige forhold, IKT-systemer, vaktordninger med mer. Dette kan eksempelvis være:

- Informasjon om systemer for oppdagelse og reaksjon.
- Lås- og adgangskontrollsystemer.
- Bygningstekniske tiltak (type dører, vinduer, transformatorceller, og andre konstruksjoner).
- Tiltak for IKT-sikring, både i forhold til hardware og software.
- Oversikt over rutiner for vaktordninger og planer for bemanning av anlegg.
- Oversikt over rutiner for innleid vekterselskap.

Enkelte deler av beredskapsplanen kan inneholde sensitiv informasjon. Dette gjelder de deler av planverket som omhandler håndtering av bevisste uønskede handlinger, for eksempel håndtering av innbrudd, sabotasje med mer.

6.2.2.5 Beredskapsrom/kommandoplasser

Dette omfatter informasjon om plassering og stedsnavn på for eksempel reservedriftssentral, samt deres funksjonsnivå, sikringstiltak og sårbarheter.

6.2.2.6 Detaljerte analyser av sårbarhet som følge av påført skade

Detaljerte analyser av sårbarhet som følge av påført skade omfatter blant annet:

- Detaljerte evalueringsrapporter.
- ROS-analyser.
- Detaljerte analyser for regional- og sentralnettet som avdekker større sårbarheter.

I mange tilfeller har offentligheten krav på innsyn etter offentleglova i evalueringsrapporter etter større hendelser. Enheten bør i slike tilfeller lage en egen offentlig rapport som ikke inneholder sensitiv informasjon om kraftforsyningen.

6.2.2.7 Reservemateriellagre og reparasjonsmuligheter

Dette omfatter informasjon om plassering av og oversikt over hvilket utstyr som er på materiallagre for større områder, samt beskrivelse av muligheter for reparasjon av kritisk utstyr og hva dette krever.

6.2.3 Viktig og sensitiv informasjon

Bestemmelsen skiller mellom viktig og sensitiv informasjon:

- Sensitiv informasjon er informasjon som kan brukes til å skade eller hindre kraftforsyningens funksjoner.

- Viktig informasjon er informasjon som er helt nødvendig for å drive, lede og gjenopprette eget kraftsystem.

For å oppfylle forskriftens krav på dette punktet bør enheten:

- Vurdere og dokumentere hvilken informasjon og ressurs som er viktig eller sensitiv for drift og sikkerhet.
- Identifisere hvor informasjonen/ressursen befinner seg (lagring, bruk, transport og liknende).
- Vurdere hvem som er rettmessig bruker av informasjonen/ressursen og hvordan denne skal være tilgjengelig for brukerne.

Enheten skal sikre at viktig informasjon er tilgjengelig også under ekstraordinære situasjoner, se § 6-3 Sikkerhetskopier.

Enheten skal til enhver tid vite hvor selskapets sensitive informasjon befinner seg. I mange tilfeller vil dette være ensbetydende med å ha egne rutiner for håndtering av sensitiv informasjon, og en bevisstgjøring av hvordan denne informasjonen skal behandles.

I forhold til hvem som er rettmessige brukere av sensitiv informasjon om kraftforsyningen, vil dette primært være selskapets egne ansatte, innleid personell etter avtale. Ved utlevering av informasjon fra egen virksomhet, er det særlig viktig å merke sensitiv informasjon. Dersom enheten må utlevere kraftsensitiv informasjon til leverandører og entreprenører som skal utføre en jobb for enheten, skal det undertegnes en sikkerhetsavtale som angitt i § 4-3 Anskaffelser i kraftforsyningen. Ved andre tilfeller, eksempelvis ved utlevering av sensitiv informasjon til utenlandske statsborgere eller virksomheter, anbefales det å ta kontakt med NVE for videre avklaring.

6.2.4 Effektiv tilgangskontroll og beskyttelse mot avlytting

Effektiv tilgangskontroll og beskyttelse mot avlytting og manipulering må ses i sammenheng med kravene til konfidensialitet, integritet og tilgjengelighet. Tiltak som vurderes for tilgangskontroll og beskyttelse bør omfatte:

- Administrative tiltak.
- Tekniske tiltak.
- Tiltak for bevisstgjøring og opplæring.
- Tiltak for å sikre effektiv tilgangskontroll og beskyttelse.

6.2.4.1 Administrative tiltak

Administrative rutiner for å sikre at kun rettmessige brukere får tilgang til sensitiv informasjon, som:

- Bruk av autorisasjonslister.
- Rutiner ved avslutting og endring av ansettelsesforhold og konsulentoppdrag.
- Rutiner for bruk av bærbare elektroniske produkter, som minnepinner, telefoner, bærbare datamaskiner og liknende.
- Regler for forsendelse av sensitiv informasjon, henholdsvis regler for bruk av e-post, brev og faks.

6.2.4.2 Tekniske tiltak

Tekniske rutiner for å skjerme sensitiv informasjon både elektronisk og på papir, som:

- Differensiert brukertilgang på server.
- Regler for passordbeskyttelse (lengde og type passord, tid for bytte av passord og liknende).
- Regler for kryptering.
- Robust systemarkitektur og konfigurasjonsstyring.
- Dokumentasjon av systemer og sikringstiltak.
- Rutiner for oppdatering og vedlikehold av sikkerhetstiltak.
- Merking av dokumenter i arkivet.
- Bruk av sertifiserte produkter, for eksempel etter Common Criteria.
- Rutiner og utstyr for beskyttelse mot ondsinnet programvare.
- Rutiner og utstyr for å oppdage, registrere og forhindre uautoriserte forsøk på inntrengning i kraftsensitive systemer og tilhørende støttesystemer.
- Bruk av inntrengningstester på kritiske systemer for å avdekke sårbarheter.
- Rutiner for logging for å avdekke uautorisert bruk av IKT-systemer. Dette gjelder for tilknytninger mot omverdenen, for eksempel internett og oppringte samband, samt nødvendig logging av intern trafikk. Enheten må kontrollere og sikre loggene, samt dokumentere resultater. Nettverkstrafikk tilkoblet kraftsensitive IT-system bør alltid logges. Se veiledning fra NorSIS om logging.
- Fysisk sikring av informasjon og IKT-systemer, samt skjerming mot innsyn.
- Rutiner for sikkerhetskopiering.
- Kontrollert avhending av informasjon og utstyr.

Se for øvrig oversikt over egnede ISO-standarder under veiledningens § 6-1 Generelt.

6.2.4.3 Tiltak for bevisstgjøring og opplæring

Tiltak for å bevisstgjøre egne ansatte om hva som er underlagt taushetsplikt, som:

- Bruk av taushetserklæringer (se egen mal for taushetserklæringer for kraftforsyningen på NVEs nettsted, www.nve.no).
- Intern opplæring og holdningsskapende arbeid med for eksempel:
  - Hvilken informasjon man ikke snakker om, og ikke utleverer.
  - Hva slags informasjon som ikke kan legges på internett.
  - Makuleringsrutiner for sensitiv informasjon.
  - Bruk av lagringsmedier med sensitiv informasjon (for eksempel minnepinner).

6.2.4.4 Tiltak for å sikre effektiv tilgangskontroll og beskyttelse

Enheten skal gjennomføre tiltak og rutiner for å sikre at beskyttelsen er effektiv. Dette kan være i form av:

- Rutiner for rapportering av sikkerhetsbrudd/sikkerhetstruende hendelser og behandling av slike rapporter.
- Periodiske egenevalueringer.
- Uavhengige, eksterne gjennomganger.
- Interne revisjoner.

6.2.4.5 Sikkerhetsinstruks

Sikkerhetsinstruksen for informasjonssikkerhet er en instruks for håndtering og beskyttelse av viktig og sensitiv informasjon, samt viktige informasjonssystemer i kraftforsyningen, både teknisk og administrativt. Sikkerhetsinstruksen bør være et resultat av tiltak som er identifiserte i den løpende helhetlige vurderingen av informasjonssikkerheten, se § 6-1 Generelt, og oppfyllelsen av denne forskriften. Videre anbefales det å ta utgangspunkt i overnevnte punkter når enheten utarbeider sikkerhetsinstruksen.

6.2.5 Inntegning på offentlig tilgjengelig kart, internett, og liknende

I det følgende er det beskrevet hvordan kraftforsyningsanlegg kan fremstilles på internett, beskrives i trykte publikasjoner og inntegnes på offentlig tilgjengelige kart i målestokk 1:10.000 – 1:1.000.000. Kart på internett der det kan zoomes inn og vise stadig flere detaljer, er ikke tillatt.

6.2.5.1 Kraftledninger

Alle kraftledninger (luftnett), uansett fysiske og elektriske egenskaper, skal ha en enhetlig utforming, markert som en enkel svart strek, eventuelt med stilisert mastesymbol. Parallelle kraftlinjer som går i samme trasé skal være inntegnet som en linje. Kabelnett i bakken inntegnes ikke. Det skal ikke benyttes symboler, farger, tekst eller tall, for å skille mellom ulike størrelser, konstruksjoner, spenningsnivå, overføringskapasiteter, tverrsnitt, antall kurser og liknende. Unntakene er:

- Fjordspenn og liknende som kan representere en fare for luftfart eller skipstrafikk skal markeres med eget enhetlig symbol for dette, eventuelt med høydeangivelse.
- Sjøkabler som kan representere en fare for skipsfarten (for eksempel ved ankring) skal markeres med enhetlig symbol, eventuelt med angivelse av dybde. Kabelendemuffer eller hus for disse skal ikke markeres.

6.2.5.2 Transformatorstasjoner, strømretter- og koblingsanlegg samt driftssentraler, IT- og sambandsinstallasjoner

Transformatorstasjoner, strømretter- og koblingsanlegg, samt driftssentraler, IT- og sambandsinstallasjoner skal ikke angis med egne symboler, herunder også opplysninger i form av navn, tekst eller tall. Dersom de likevel må markeres, skal symbol for hus eller bedrift benyttes, uten symbolikk for faktisk form, størrelse eller utstrekning. Antennemaster som kan representere en fare for lufttrafikken markeres med enhetlig symbol og høyde.

6.2.5.3 Kraftstasjoner

Kartseriens innarbeidete enhetlige symbol benyttes. Plassering av bygninger, koblingsanlegg og liknende, samt øvrige opplysninger i form av tall eller tekst, skal unngås. Det er ikke tillatt å vise detaljer som kabelhus/-føringer, ventilasjonssjakter/-hus, tverrslag/-porter og liknende.

6.2.5.4 Dammer/magasiner

Innarbeidet symbol for dam (tykk svart strek) benyttes, eventuelt med navn. Det skilles ikke mellom ulike konstruksjonstyper. Det er ikke tillatt å angi detaljer som luker, omløpstunneler, nødtappeløp, sprengbare felt og liknende. Inntak kan angis på kart.

Vanlige opplysninger om magasiner som høyeste regulerte vannstand (HRV), laveste regulerte vannstand (LRV) og vanndybder kan angis.

6.2.5.5 Utendørs merking i kraftforsyningsanlegg

Anlegg og avganger bør ikke merkes slik at det er lett synlig for uvedkommende.

§6-3 Sikkerhetskopier

Det skal til enhver tid foreligge oppdaterte sikkerhetskopier av informasjon og programvare som er av betydning for kraftforsyningens drift og sikkerhet. Herunder skal all nødvendig informasjon og programvare sikres med fjernlagring av sikkerhetskopier.

Nødvendig dokumentasjon om kraftsystem og anlegg som lagres på datamedia skal også foreligge som utskrifter. Disse skal oppdateres årlig og oppbevares på et sikkert sted.

Veiledning

6.3.1 Rutiner og kvalitet

Hensikten med kravet om sikkerhetskopier er å sikre at viktig informasjon for kraftforsyningens drift, gjenoppretting og sikkerhet er tilgjengelig til enhver tid ved behov. Dersom viktig informasjon (dokumenter, data og programvare) går tapt, blir feilaktig eller mangelfull, må det finnes oppdaterte sikkerhetskopier.

Enheten bør etablere dokumenterte systemer og rutiner for sikkerhetskopiering. Rutinene må også beskrive hvordan og hvor hyppig sikkerhetskopien skal oppdateres. Enhetens ROS-analyse skal være basis for å avgjøre omfang, hyppighet, oppbevaringstid og lagringssted, men enheten må også vurdere dette fortløpende. Enheten bør ha planer for gjenoppretting etter havarier og skader på informasjonssystemene.

Sikkerhetskopiene skal inneholde programvare, dokumentasjon om programvare, konfigurasjonsdata og informasjon fra viktige IT-systemer for drift, sikkerhet og gjenoppretting av kraftforsyningen. Nødvendig programvare og utstyr bør være tilgjengelig, slik at gjenoppretting av viktig informasjon er praktisk mulig, også etter et totalhavari. Lagringsformat bør være slik at informasjonen lar seg gjenopprette selv om det opprinnelige utstyret det er lagret på (både maskinvare og programvare) blir skadet eller er utilgjengelig.

6.3.2 Oppbevaring og papirkopier

Enheten må oppbevare alle sikkerhetskopier på en måte som forebygger og forhindrer tap og skade, samt sikrer tilgjengelighet. Kun autorisert personell skal ha tilgang til sikkerhetskopiene. Sikkerhetskopiene skal være sikret mot tyveri og skade, og bør lagres i brannsikkert og avlåst sikkerhetsskap. Enheten må fjernlagre sikkerhetskopier, slik at ikke samme hendelse medfører at både original og sikkerhetskopier blir helt eller delvis utilgjengelige. Med fjernlagring menes at sikkerhetskopiene lagres i et bygg/anlegg som er fysisk atskilt fra bygget originalene oppbevares i. Sikkerhetskopier av programvare og elektronisk lagrede data bør testes regelmessig for å sikre at man kan gjenopprette og tilbakelegge programvare/data.

Hensikten med kravet om å oppbevare utskrifter er å sikre tilgjengelighet og kontinuitet dersom elektronisk lagrede utgaver er utilgjengelige (svart nett og skadete IT-systemer). Det skal til enhver tid foreligge papirkopier av de mest vitale opplysningene om kraftforsyningsanlegg og kraftsystem. Disse kan benyttes dersom IT-systemene blir utilgjengelige over lengre tid. Med vitale opplysninger menes informasjon som er nødvendig for å kunne drifte og gjenopprette kraftforsyningen. Enheten må lagre papirkopiene på et sikkert sted, samt oppdatere dem årlig og ved større endringer.

§6-4 Særlige krav til driftskontrollsystemer

Driftskontrollsystemer omfatter driftssentraler, sambandsanlegg og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner.

a) Planer og dokumentasjon

Alle enheter i KBO skal til enhver tid ha oppdatert dokumentasjon over de eksisterende og planlagte driftskontrollsystemer.

b) Tilgangskontroll

Alle driftskontrollsystemer skal ha kontrollordninger som effektivt beskytter mot intern og ekstern uautorisert fysisk og elektronisk tilgang og spredning av ondsinnet programvare og lignende.

c) Systemsikkerhet

Driftskontrollsystem i klasse 2 skal utføres med redundans frem til det enkelte kraftforsyningsanlegg i klasse 2 og 3, slik at ikke viktige funksjoner tapes på grunn av feil eller enkelthendelse.

Driftskontrollsystem i klasse 3 skal utføres med full redundans i hele systemet frem til det enkelte kraftforsyningsanlegg i klasse 2 og 3, og til andre relevante driftskontrollsystemer i klasse 2 og 3, slik at en feil eller enkelthendelse ikke kan sette viktige funksjoner ut av drift. Redundansen skal utføres med fysisk og elektronisk separering. Driftskontrollsystemet skal utføres så robust at funksjon også opprettholdes under store og langvarige påkjenninger. Driftskontrollsystemer i klasse 3 skal kunne fungere uavhengig av offentlige nett og teletjenester.

Driftskontrollsystemer i klasse 2 og 3 og annet samband av betydning for kraftforsyningens drift og sikkerhet skal minimum ha to fysisk atskilte og uavhengige sambandsveier til kraftforsyningsanlegg i klasse 2 og 3.

d) EMP og EMI beskyttelse

Driftssentraler, annen kontrollutrustning og sambandsinstallasjoner i klasse 2 og 3 skal beskyttes mot elektromagnetisk puls (EMP) og elektromagnetisk interferens (EMI).

e) Brannsikkerhet

Automatisk brannalarm skal installeres i alle rom i den delen av bygget hvor driftssentralen med tilbehør er installert. Denne skal også varsle eventuell hjemmevakt.

f) Beredskapsrom

Alle driftssentraler i kontrollsystem klasse 3 skal ha beredskapsrom for ledelse og driftspersonell. Norges vassdrags- og energidirektorat kan vedta om driftssentraler i kontrollsystem klasse 1 og 2 skal ha beredskapsrom. Beredskapsrom skal tjene som nøddriftssentral og understøtte andre ledelsesfunksjoner i ekstraordinære situasjoner, samt gi personell beskyttelse

Veiledning

Pålitelige driftskontrollsystemer har avgjørende betydning for sikker ledelse og drift, effektiv håndtering av ekstraordinære situasjoner og rask gjenoppretting av funksjon. I tillegg må viktige driftskontrollsystemer virke selv ved langvarige og ekstraordinære påkjenninger.

Denne bestemmelsen er krav til dokumentasjon, tilgangskontroll, systemsikkerhet, samt til beskyttelse av driftspersonell og utstyr i driftskontrollsystemene.

Bestemmelsen fastsetter videre særlige krav om informasjonssikkerhet som gjelder for driftskontrollsystemer. Bestemmelsene må leses i sammenheng med §§ 6-1 Generelt, 6-2 Beskyttelse av informasjon og 5-5 Sikringsnivå. Det er viktig å understreke at enheten står fritt til å velge andre løsninger enn de eksempler som er gitt i denne delen av veiledningen, så lenge valgt løsning gir samme funksjonalitet, eller bedre.

Forskriftens bestemmelser gjelder for alle ledd i hele systemet som er nødvendige for å ivareta driftskontrollfunksjonene som definert i § 6-1 b. Bestemmelsen gjelder for driftssentral og kontrollsystem inkludert samband for signaloverføring og tale, helt ut til de kontrollerte kraftforsyningsanlegg med alle nødvendige støttefunksjoner. Støttefunksjonene kan være IKT-utstyr, nødstrøm, ventilasjon og kjøling av datarom.

Vedrørende sikkerhetskrav og analyse, se § 6-1 Veiledning.

6.4.1 Planer og dokumentasjon

Planlegging og dokumentasjon er nødvendige hjelpemidler for å oppnå en rasjonell utvikling av driftskontrollsystemet innen et selskap, ivareta sikkerheten, og kunne dokumentere dette.

Hver KBO-enhet skal utarbeide en plan som fremlegges i forbindelse med melding om nybygg, ombygninger og liknende, og ellers når NVE ber om det. Planen bør gis en vid tidshorisont, opp til 10 år. Planen skal inneholde en beskrivelse av virksomhetens ambisjonsnivå, tidshorisonter for større vedlikeholdsarbeid eller nyanskaffelser, oversikt over dagens system og bruksområder samt en vurdering av dagens og fremtidig IKT-sikkerhetsnivå. Planen og dens forutsetninger bør jevnlig vurderes.

Virksomheten skal til enhver ha oppdatert dokumentasjon over eksisterende driftskontrolløsninger, inkludert sikkerhetstiltak etter beredskapsforskriftens krav.

Alle planer og dokumentasjon skal inngå i virksomhetens kvalitetssystem.

6.4.1.1 Sikkerhetspolicy

Både for utformingen av driftskontrollsystemet og for driften av dette, bør det utformes en samlet sikkerhetspolicy med beskrivelse av risiko, krav, tiltak og liknende. Denne bør minst inneholde:

- Virkeområde og avgrensing.
- Ansvarsforhold og organisering.
- Vurdering av trusler (risiko- og sårbarhet).
- Inndeling i sikkerhetssoner, fysisk og virtuelt.
- Krav til kontroll med eksterne forbindelser, tilgang og kommunikasjon.

- Nettverk og konfigurasjonskontroll.
- Autorisasjon av og krav til rettmessige brukere.
- Administrasjon av ulike brukergruppers rettigheter, passord og liknende.
- Krav til og avtaler med leverandører.
- Sikkerhetskopiering og forsvarlig sletting av sensitiv informasjon.
- Driftssikkerhet, drifts- og sikkerhetsinstruks.
- Testing, overvåkning og kontroll av sikkerhet.
- Beredskapsplan og krav til gjenoppretting av funksjon, må også inneholde planer for de mest ødeleggende scenarioer.
- Håndtering av hendelser, sikkerhetsbrudd og ekstraordinære situasjoner.
- Rutiner for evaluering, rapportering.

For andre viktige områder innen informasjonssikkerhet vises det til nasjonale eller internasjonale standarder, se § 6-1.8 Henvisninger.

6.4.1.2 Systembeskrivelse og konfigurasjonskontroll

Av hensyn til analyse, planlegging og løpende vurdering av sikringstiltak (fysisk sikring og tilgangskontroll), samt god evne til rask gjenoppbygging, er det viktig at driftskontrollsystemet til enhver tid er godt beskrevet med komplett dokumentasjon, gjerne på flere nivåer (systemoversikt, delsystemer og konfigurasjonsdetaljer). Rask tilgjengelighet til oppdatert systeminformasjon vil også kunne være helt avgjørende ved en hendelse. Oppdatert systembeskrivelse er et godt grunnlag for å vurdere konsekvenser, tilgang på reservemateriell, mulige reserveløsninger og andre beredskapstiltak. Det er derfor viktig at dokumentasjonen utformes med tanke på slik bruk.

6.4.2 Tilgangskontroll

Tilgangskontroll omfatter både fysisk, elektronisk og administrativ sikkerhet. Det skal etableres effektive tiltak mot alle former for uautorisert adgang, inntrenging og angrep på stedet, eller via kommunikasjon, spredning av uautorisert eller ondsinnet programvare og liknende og skal sikre;

- Tilgjengelighet til utstyr, prosesser og funksjoner i driftskontrollsystemet for autoriserte brukere i henhold til tjenstlig behov og til rett tid.
- At informasjon som behandles (opprettes, lagres, endres og slettes) og kommuniseres i driftskontrollsystemet opprettholder nødvendig integritet og konfidensialitet slik at driftskontroll kan utøves pålitelig.
- At informasjon som kommuniseres i, til og fra driftskontrollsystemet opprettholder nødvendig integritet og konfidensialitet slik at informasjonen er pålitelig og etterrettelig.
- At driftskontrollsystemets utstyr og prosesser opprettholder forutsatt funksjonalitet.

Tilgangskontrollen skal hindre eller redusere risikoen for:

- Uautorisert fysisk tilgang. Kun driftspersonellet og andre autoriserte skal ha tilgang til driftskontrollsystemets utstyr, nøkler, adgangskort og liknende.
- Uautorisert elektronisk tilgang. Egne ansatte, innleid personell eller eksterne personer skal ikke ha tilgang til elektroniske driftskontrollsystemer eller prosesser utover tjenstlig behov. Andre IKT-systemer skal ikke ha unødig tilgang til eller

uautorisert kommunikasjon med driftskontrollsystemer. Systemene skal forøvrig sikres mot datainnbrudd etter § 6-2 Beskyttelse av informasjon.

- Spredning av ondsinnet programvare og liknende. Driftskontrollsystemer skal sikres mot at ondsinnet programvare kan medføre en trussel mot systemene.

Tilgangskontroll skal implementeres for fysiske enheter, elektroniske systemer og dokumentasjon.

6.4.2.1 Intern og ekstern tilgang

Ekstern tilgang er tilgang til driftskontrollsystemet utenfor det området som er fysisk kontrollert av eier. For eksempel kommunikasjonstilkopling via privat eller offentlig datanettverk og avlytting av radiobasert samband.

Intern tilgang er tilgang til driftskontrollsystemet innenfor det området som er fysisk kontrollert av eier. For eksempel tilgang til driftskontrollfunksjoner via virksomhetsinternt datanettverk og adgang til utstyr i driftskontrollsystemet.

6.4.2.2 Kontrollordninger

Kontrollordninger omfatter administrative og tekniske rutiner og tiltak. Eksempler på administrative rutiner og tiltak er passordrutiner, autorisasjon av brukere, konfigurasjonskontroll av utstyr/programvare og sikkerhetsavtaler med leverandører. Eksempler på tekniske rutiner og tiltak er adgangskontrollsystem, autentisering av brukere/utstyr, brannmurer i nettverk, logging, fysisk sikring av utstyr og bruk av programvare for viruskontroll.

6.4.2.3 Beskyttelse

Beskyttelse innebærer at driftskontrollsystemene skal ha fysisk og elektronisk beskyttelse mot uautorisert tilgang som kan true driftskontrollsystemets funksjoner med hensyn til tilgjengelighet, integritet og konfidensialitet.

Det understrekes at sikkerhetsnivået etter dette punktet ikke bare avhenger av vedkommende driftskontrollsystems egen klasse, men like mye etter hvilke andre system det er tilknyttet. For eksempel kan bruk av offentlige ekomtjenester eller tilkoblinger til kommunikasjonsnett utenfor eget sikkerhetsområde, eksponere enheten for uautorisert snoking/inntrengning og spredning av ondsinnede program.

Driftskontrollsystemet skal ikke ha tilgang som medfører at utgående dataforbindelser til internett kan etableres fra driftskontrollsystemet. Dette er viktig for å forhindre at ondsinnet programvare i driftskontrollsystemet kan utnytte slike dataforbindelser. For tiltak - se eget punkt om logisk skille, brannmurer og liknende i veiledningen.

Systemer for overordnet kraftsystemkontroll, produksjonsplanlegging og kraftbørshandel er eksempler på systemer som kan være tilknyttet enhetens driftskontrollsystem. Systemer for å realisere Smart Grid og Avanserte Måle- og styringssystemer (AMS) vil kunne medføre økt behov for tilgang til og integrasjon med informasjon og funksjonalitet i driftskontrollsystemet. For alle slike systemer der slik utvidet tilgang er aktuelt skal enheten minst gjøre en særskilt og grundig vurdering av trusselnivå og risiko for uautorisert tilgang via slike systemer før tilgang eventuelt gis. Det forutsettes også at kontrollordninger ved slik tilgang gir minst like god beskyttelse som denne forskriften krever.

Enheten skal til enhver tid ha dokumentert oversikt over alle punkter der fysisk eller elektronisk tilgang til driftskontrollsystemet er tilgjengelig. For alle slike tilgangspunkter skal det etableres og dokumenteres tilgangskontroll i form av fysisk og/eller elektronisk beskyttelse, samt operative og administrative rutiner for autorisert bruk. Det bør regelmessig, minst årlig for anlegg i klasse 2 og 3, gjennomføres uavhengige gjennomganger eller revisjoner av tilgangskontrollen for å kontrollere at beskyttelsen er tilstrekkelig og effektiv. Det forutsettes jevnlige gjennomføringer av internrevisjon. Tilgangskontroll bør minst vurderes og kontrolleres ved alle endringer som omfatter utstyr med slike tilgangspunkter eller når autorisert bruk av tilgangspunktene endres.

6.4.2.4 Fysisk beskyttelse

Fysisk beskyttelse skal sikre at uvedkommende ikke har fysisk tilgang som kan føre til uautorisert bruk, misbruk, skade eller ødeleggelse av driftskontrollsystemets utstyr eller funksjoner.

- For fysiske sikringstiltak for driftskontrollsystemer, se § 5-5 Sikringsnivå om driftssentraler med tilhørende bygg og sambandsanlegg spesielt.
- For generell adgangskontroll til anlegg, se § 4-5 Adgangskontroll
- For besøksrestriksjoner, se § 4-6 Besøksrestriksjoner

Ved driftssentraler skal det etableres særlige adgangskontrollerte soner – se eget punkt nedenfor. De deler av anlegg og utstyr som er uten løpende tilsyn, skal holdes avlåst. Det skal føres jevnlig kontroll med kabelføringer og andre steder hvor fysisk adgang kan gi elektronisk tilgang til systemet.

Krav til adgangskontroll - driftssentraler

For driftssentraler med tilhørende utrustning skal det etableres egen adgangskontrollert sone, i henhold til § 4-5 Adgangskontroll.

Driftssentraler med tilhørende utrustning inkluderer:

- Driftssentraler, sambandsanlegg og øvrige anlegg og komponenter som ivaretar driftskontrollfunksjoner.
- 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 styring av koblinger og overvåking av tilstand i anleggene.
- Utstyr for hjemmevakt og fjerntilgang for leverandør med tilgang for utøvelse av driftskontroll, IKT-drift eller leverandørstøtte i driftskontrollsystemet.

Om håndtering av adgangskontrollert sone for hjemmevakt og fjerntilgang utenfor etablert sone – se eget veiledningspunkt nedenfor.

Rom som inneholder driftssentraler med tilhørende utrustning skal være egne adgangskontrollerte sikkerhetssoner. Enheten må holde disse rommene avlåst for alle som ikke har selvstendig adgang. Personer kan få selvstendig adgang gjennom autorisering. Øvrige skal ledsages av personer som har gyldig autorisasjon. Dersom enheten har stasjonært eller bærbart utstyr som kan brukes til styring og kontroll av kraftsystemkomponenter utenfor driftssentralen, for eksempel på eget kontor, skal enheten sikre disse rommene og omgivelsene tilsvarende. De samme kravene gjelder for lokaler der det oppbevares utstyr for autorisert tilgang for IKT-drift eller leverandørstøtte i driftskontrollsystemet.

Ved sambandsanlegg kan det være aktuelt med tilgang for flere etater og brukergrupper. Andre brukeres adgang til anlegg og rom av betydning for kraftforsyningen skal være regulert i egne avtaler/instrukser og begrenses til tjenstlig behov.

Figur 3: Prinsipp for adgangskontroll

Sikkerhetssonen skal være utstyrt med adgangskontrollsystemer av en slik kvalitet at de ikke kan forseres uautorisert uten at det foretas et synlig innbrudd. For veiledning om fysiske barrierer, se § 5-5 Sikringsnivå, spesielt om skallsikring og sonesikring.

Det bør ikke være luftedør i driftssentralen. I tilfelle må det etableres sikringstiltak ved og rundt driftssentralen som oppfyller kravene til egen adgangskontrollert sone.

6.4.2.5 Elektronisk beskyttelse

Driftskontrollsystemer skal sikres med elektronisk tilgangskontroll av høy kvalitet, slik at det ikke er mulig for uvedkommende og uautoriserte å skaffe seg tilgang til driftskontrollsystemer via enhetens egne eller eksterne IT-systemer og samband (elektronisk kommunikasjon). Dette gjelder uansett hvem som eier eller driver, produserer eller formidler ulike systemer, nett eller tjenester, og uansett om de er fysiske, virtuelle, faste eller trådløse. Datasystemene skal sikres med tilgangskontroller av tilstrekkelig høy kvalitet. Det er nødvendig å skille ekstern uautorisert datatrafikk fra kraftforsyningens vitale kontroll- og datasystemer. Dette kan løses ved fysisk eller elektronisk atskillelse, eventuelt bruk av kraftige logiske skiller og sikkerhetsmekanismer som for eksempel kombinasjoner av riktig oppsatte rutere, "brannmurer" og automatiske overvåknings-/alarmsystemer, med mer.

For å oppfylle beredskapsforskriftens krav til elektronisk tilgangskontroll er den sikreste metoden å holde driftskontrollsystemet atskilt fra andre systemer, fysisk/elektronisk skille. Dette oppnås ved at minst ett av følgende er oppfylt:

- Fysisk atskillelse, ingen form for forbindelser mot driftskontrollsystemet.
- Elektronisk atskillelse, slik at ikke uvedkommende elektronisk kommunikasjon kan hoppe, smitte, spre seg eller liknende fra andre systemer til driftskontrollsystemet, eller manipuleres til slikt av uvedkommende.

For kontroll av restrisiko må det også minst føres kontroll med / logging av intern trafikk, samt gjennomføres konfigurasjonskontroll med systemet, se egne punkter nedenfor om logging og overvåkning samt programfeil-/svakheter og bakdører.

Der flyttbare lagringsmedia (for eksempel minnepinner) benyttes for overføring av data mellom driftskontrollsystemet og andre systemer, må det minst være kontrolltiltak som forhindrer overføring av uautoriserte data, inklusive ondsinnet programvare.

6.4.2.6 Interne datanettverk og samband, spesielle momenter

Krav for tilgangskontroll omfatter også tilkopling til lokalt datanett for kontrollanlegg i kraftforsyningsanlegg som styres via et sentralt driftskontrollsystem. Krav til og tiltak for sikker lokal- og fjerntilgang for kontrollanlegg må derfor vurderes på linje med driftskontrollsystemets tilgangskontroll.

Det skal normalt ikke tillates bruk av trådløse nettverk (eksempelvis WLAN) eller IT-utstyr som inneholder trådløse sendere gjennomgående i driftskontrollsystem. Enheten bør heller ikke tillate trådløs kommunikasjon i lokale kontrollanlegg. Årsaken er sårbarheten i forhold til blokkering av radionett, eksponering for trusler i form av inntrengning og interferens som setter integritet og konfidensialitet for informasjon som overføres, i fare. Uautorisert bruk av tilgjengelige trådløse sendere er vanskelig å detektere og kontrollere. Derfor er risikoen svært høy for at uautoriserte får tilgang til driftskontrollsystemet ved hjelp av ondsinnet programvare.

For klasse 1 anlegg kan bruk av trådløse nettverk tillates etter særskilt risikovurdering. I risikovurderingen må man også vurdere risikoen for forstyrrelser på radionettet. Det forutsettes at ekstra sikkerhetstiltak, som for eksempel forsterket kryptering, benyttes. Risikovurderingen skal dokumenteres.

For klasse 2 og 3 tillates det ikke bruk av trådløse datanettverk i driftskontrollsystemet. Enheten bør også påse at utstyret som benyttes ikke inneholder sendere/mottakere for trådløs kommunikasjon. Unntaket er om enheten etter særskilt vurdering har behov for trådløs kommunikasjon mot mindre viktige komponenter. Før dette tillates skal en risikovurdering utføres. Vurderingen skal belyse konsekvensen ved at komponenten blir utilgjengelig ved at det trådløse nettverket faller ut eller blir kompromittert, samt risikoen for inntrengning og manipulering av driftskontrollsystemet via det trådløse nettverket. Dette skal dokumenteres. Det forutsettes også her at ekstra beskyttelsestiltak som forsterket kryptering, signalbegrensninger, utstyrsautentisering og andre aktuelle sikkerhetsmekanismer brukes. Minst ett kommunikasjonsalternativ som skal fungere som redundans skal ikke innbefatte noen form for trådløst nettverk.

For viktige radiobaserte samband bør sårbarhet i forhold til tilgjengelighet, samt eksponering for trusler mot integritet og konfidensialitet vurderes særskilt. For slike samband bør ekstra beskyttelsestiltak som forsterket kryptering, utstyrsautentisering og andre aktuelle sikkerhetsmekanismer brukes.

Merk også at sambandssystemer ofte inneholder programvarestyrte komponenter med elektronisk tilgang for drifts- og vedlikeholdsfunksjoner i delsystem for samband (for eksempel rutere og svitsjer). Det er viktig at kontrolltiltak for sikker lokal- og fjerntilgang for disse vurderes på linje med driftskontrollsystemets øvrige komponenter.

6.4.2.7 Logisk skille, brannmur og liknende

Analyse av hvordan driftskontrollsystemet og øvrige ressurser skal beskyttes Full fysisk eller elektronisk atskillelse kan i mange tilfeller gi utilstrekkelig funksjonalitet. Alternativt kan den elektroniske tilgangskontrollen utføres som et kraftig ”logisk skille” med full kontroll av all kommunikasjon. Dette kan gjøres ved hjelp av en såkalt ”brannmur”. En ”brannmur” er langt mer enn kun å installere en brannmurmaskin, det er en funksjon. For at en ”brannmur” skal kunne oppfylle beredskapsforskriftens krav, må minst følgende være på plass:

- Strategi for den beskyttelse som skal oppnås, og hvordan dette skal gjennomføres.
- Plan for hele det elektroniske nettverket/arkitektur med full kontroll over alle eksterne og interne forbindelser (eksempelvis krav til ”single entry”).
- Plan, anskaffelse, installasjon og riktig konfigurasjon av maskin- og programvare
- Administrative rutiner og oppfølging.
- Annet relevant som fremkommer av enhetens ROS-analyser for driftskontrollsystemet.

En brannmur må minst ivareta følgende funksjoner:

- Sperre for alle tjenester og annet som ikke eksplisitt tillates gjennom brannmuren.
- Avvise alle forsøk på uautorisert tilgang.
- Rute alle eksterne linjer til et avgrenset og kontrollert område, som ikke inneholder sensitiv informasjon eller viktig ressurser.
- Logge all aktivitet over eksterne forbindelser.
- Kontrollere all mottatt informasjon for virus og annen ondsinnet programvare.
- Kontrollere adresser, protokoller, identiteter og eventuelt integritet og autentisering.

Ved større driftskontrollsystemer/nettverk kan summen av krav til sikkerhet, funksjonalitet og kapasitet, gjøre det nødvendig å dele nettverk og maskiner i flere områder/soner (såkalt Demilitarized Zone, DMZ). Slike soner kan ha ulike krav til tilgangskontroll ut fra ulike krav til beskyttelse. Tilgangen til og fra hver sone kan da kontrolleres av en separat brannmur for hver sone. Se litteratur for dette under henvisninger.

For å ivareta sikkerheten i nettverk er bruk av rutere og liknende et viktig og nødvendig, men ikke tilstrekkelig tiltak alene. De må minst inngå i en kombinasjon med ovennevnte brannmurfunksjon. En løsning kan være å legge en ekstern ruter (”grovsorterer”) foran brannmuren og en eller flere interne rutere etter brannmuren.

6.4.2.8 Logging og overvåking

Ved alle dataanlegg som omfattes av beredskapsforskriftens krav til tilgangskontroll skal det føres logg over relevante aktiviteter, særlig ved eksterne forbindelser til driftskontrollsystemer. Det må minst etableres rutiner som kan avdekke uautorisert tilgang, bruk, eller forsøk på dette. Dette kan for eksempel realiseres ved å tilpasse loggsystemene.

Ved større og viktige systemer kan det være behov for mer aktiv og forebyggende overvåkning. Da bør det installeres automatisk overvåkningssystem (Intrusion detection system -IDS), som automatisk registrerer og alarmerer forsøk på inntrengning, sniffing og annen uautorisert virksomhet.

I tillegg må enheten minst etablere effektive reaksjonsrutiner for å håndtere alarmer og uønskede hendelser. Enheten bør vurdere å installere automatisk beskyttelsessystem (Intrusion protection system -IPS), sammen med IDS. IPS kan automatisk isolere programmer, data, maskiner eller deler av nettverk for å begrense mulige skadevirkninger ved uautorisert tilgang. Enheten må være oppmerksom på at automatiske systemer som slår av nødvendige funksjoner, kan medføre uønskede effekter i forhold til driftskontroll. Dersom enheten velger slike systemer, bør denne problemstillingen derfor vurderes nøye sammen med leverandørene.

6.4.2.9 Tilgang for autoriserte brukere

Personer med tjenestelig behov skal autoriseres for å få tilgang til driftskontrollsystemene. Rutiner for autorisering skal være beskrevet. For å skille mellom autoriserte og uautoriserte/uvedkommende brukere, må det både for intern og ekstern tilgang minst dokumenteres rutiner og tiltak for:

- kontroll med autorisering av rettmessige brukere.
- autentisering av rettmessige brukere (passord, biometri og smartkort eller kombinasjoner).
- å sikre at autentiseringen er tilstrekkelig, eksempelvis kontroll av passord (lengde, innhold) og/eller samtidig bruk av to autentiseringsløsninger ved pålogging.
- å skifte passord.
- å sikre at utstyr som forlates ikke skal kunne brukes av uvedkommende (avlogging).
- å differensiere autoriserte brukeres ulike rettigheter ved tilgang (tilgang til eksempelvis å lese, endre, koble) i henhold til tjenstlige behov.

Det er viktig at ulike brukergruppers tjenstlige behov for tilgang til ulike delsystemer og funksjoner i driftskontrollsystemet kan ”skreddersys”. Det er et naturlig skille i tjenstlig behov mellom tilgang for:

- Sikkerhetsadministrator; administrasjon av sikkerhetsfunksjoner og systemrettigheter i utstyr og prosesser (eksempelvis tilgangskontroll).
- Driftsoperatør; operativ bruk av driftskontroll (driftsoperatørs bruk av SCADA funksjoner for prosesskontroll i kraftforsyningsanlegg inklusive styring, overvåkning og feilsøking).
- IKT-driftspersonell; overvåkning, feilsøking og gjenoppretting i driftskontrollsystemets IKT-baserte utstyr og prosesser.

Innen hver av disse gruppene vil det kunne være ulike undergrupper på forskjellig nivå med spesifikke behov for operativ og administrativ tilgang.

For egne ansatte bør autorisering og tildeling/endring/inndragelse av tilgangsrettigheter være regulert i dokumenterte prosedyrer og retningslinjer. Ved oppsigelse eller endring i tjenesteforhold er det spesielt viktig å ha gode rutiner for dette.

For eksterne brukere må tilgangsrettighetene som et minimum avtalefestes. Som hovedregel skal ikke funksjoner for sikkerhetsadministrator og driftsoperatør kunne utøves av eksternt personell. Unntak fra dette kan være aktuelt der flere enheter benytter et felles driftskontrollsystem. Tilgang for eksternt personell bør alltid tidsbegrenses. Avtaler om tilgang for eksterne må minst inneholde bestemmelser om regelmessig behovsvurdering av tilgang, samt fornying av tilgangsrettigheter.

Enheten skal kartlegge og ha oversikt over operative og sikkerhetsmessige krav til styring av tilgang. For å oppnå optimal styring av tilgang bør enheten ha god oversikt over og kompetanse på funksjonalitet i driftskontrollsystemets aksessrettigheter i ulike delsystemer på utstyr og prosessnivå. Slik informasjon er også et nødvendig underlag i anskaffelsesprosessen for systemer som inngår i driftskontrollsystemet for å sikre at ulike aksessrettigheter er tilgjengelige i henhold til enhetens behov.

6.4.2.10 Autentisering ved tilgang (innlogging)

All autentisering av brukere ved tilgang (innlogging) må benytte sikkerhetsmekanismer med tilstrekkelig høy kvalitet og beskyttelse som sikrer integritet og konfidensialitet i disse. All autentisering av brukere skal entydig identifisere person.

Enheten kan velge å benytte systemer for tilgangskontroll basert på to-nivå autentisering med bruk av engangspassord (passordgenerator som genererer nye passord hver gang). Dette skal benyttes for autentisering ved fjerntilgang, men bør også vurderes for autentisering generelt. Mange vil være kjent med slike systemer gjennom bruk av nettbank.

For autentisering basert på bruk av passord som kan brukes flere ganger, bør enheten ha rutiner og tiltak som sikrer at passord endres jevnlig, at de ikke utformes slik at de er lette å knekke.

For eldre driftskontrollsystemer der det ikke er mulig å ha autentisering som entydig identifiserer enkeltpersoner, kan det tillates å benytte fellesbrukere med felles passord. I slike tilfeller skal enheten ha rutiner for å:

- Sikre at fellespassord endres før nytt utstyr tas i bruk.
- Registrere tilgang til fellespassord (kun autorisert personell med strengt tjenestelige behov).
- Sikre jevnlig endring av fellespassord.

Enheten skal kun tillate bruk av felles passord innenfor særskilt adgangskontrollert sone.

6.4.2.11 Fjerntilgang, hjemmevakt

Behovet for tilstandsovervåkning og kopling samt feilretting i driftskontrollsystemet fra hjemmevakt må vurderes strengt. Enheten skal ha kontrollordninger for hjemmevakt som tilsvarer et beskyttelsesnivå lik det som finnes for styrings- og kontrollfunksjonene som utføres fra virksomhetens driftsentral eller øvrige lokaler. Sambandsvei mellom utstyr hos hjemmevakt og driftskontrollsystem skal oppfylle alle krav til systemsikkerhet på lik linje med øvrige samband i driftskontrollsystemet.

Fjerntilgang fra hjemmevakt for driftskontrolloperatører

For bruk av hjemmevakt med tilgang til driftskontrollsystem for operatører skilles det mellom driftskontrollsystemer med og uten døgnbemannet driftssentral;

- For driftssentraler i klasse 3 er det ikke tillatt med tilgang fra hjemmevakt. Disse driftssentralene skal være døgnbemannet. For tilgang til IKT-driftspersonell som skal bistå med feilretting i driftskontrollsystemet – se nedenfor.
- For driftssentraler i klasse 2 kan hjemmevakt ha tilgang til driftsstatus og alarmer. Mulighet for kobling i klasse 2-anlegg tillates ikke. Det skal kun skje fra operatørrommet i driftssentralen. Koblinger i klasse 1-anlegg i distribusjonsnettet tillates fra hjemmevakt-pc.
- For driftssentraler i klasse 1 kan hjemmevaktordning med mulighet for kobling i distribusjonsnettet tillates.

Fjerntilgang fra hjemmevakt for eget IKT-driftspersonell

Fjerntilgang fra hjemmevakt for IKT-drift skal vurderes restriktivt på linje med hjemmevakt for driftsoperatør. I de tilfellene virksomheten vurderer det som nødvendig å benytte fjerntilgang til driftskontrollsystemet skal oppkobling være strengt regulert.

For oppkobling mot klasse 3 driftskontrollsystem gjelder følgende;

- Det skal være høyt sikringsnivå rundt oppkobling og arbeid i driftskontrollsystemet fra hjemmevakt-pc. Det skal være utarbeidet en egen risiko- og sårbarhetsanalyse for dette. I analysen skal behov, trusler (både interne og eksterne forhold), sårbarhet, og effektivitet av iverksatte tiltak vurderes.
- Basert på blant annet risikoanalysen skal det utarbeides sikkerhetsrutiner for oppkobling. fra hjemmevakt-pc.
- All oppkobling fra hjemmevakt skal kun skje etter tillatelse fra driftsentralen i hvert enkelt tilfelle. Oppkoblingen skal logges.
- Oppkobling med hjemmevakt-pc skal bare skje dersom det er absolutt behov for det og feilen i driftskontrollsystemet er av en slik art at det er fare for forsyningssikkerheten.
- IKT-driftspersonell skal kun ha begrensede tilgang til funksjoner for styring og kontroll av utstyr og prosesser. Eksempler er innhenting av status, feilsøking, feilretting av systemet, logging og omstart.
- IKT-driftspersonell skal kun få tilgang til driftsstatus for kraftsystemet eller alarmer dersom feilsøkings- og feilrettingsarbeidet krever det.
- IKT-driftspersonell skal ikke kunne foreta koblinger i kraftsystemet.
- Terminering av oppkobling skal kunne skje fra driftsentralen.
- Dersom personen som skal koble seg opp mot driftskontrollsystemet befinner seg et annet sted enn hjemme, for eksempel på et offentlig sted, skal man være ekstra restriktive med tillatelse til oppkobling. Sikkerhetsinstruksen skal omhandle dette spesielt. Her gjelder samme krav til beskyttelse som i § 6-2 ”Beskyttelse av informasjon”.
- Utstyr for hjemmevakt-pc skal kun ha nødvendig maskin- og programvare for autorisert tilgang og funksjon mot driftskontrollsystemet. Det er ikke tillatt å benytte hjemmevakt-pc for andre formål, som for eksempel lokal bruk av internett eller e-post. Slik bruk skal kun skje via sikret kommunikasjonskanal og

ha sikker bruk på lik linje som når tilkobling skjer innenfor virksomhetens egne lokaler.

- Oppkobling skal skje via sterk bruker- og utstyrsautentisering som innebærer minimum to-nivå-autentisering av brukere ved bruk av engangspassord samt bruk av sikker kanal gjennom brannmur for kommunikasjon. Et eksempel er Virtual Private Network (VPN) med sterk kryptering av forbindelse. Krypteringen skal også omfatte eventuelt trådløst nettverk.
- Virksomheten bør vurdere bruk av IDS eller IPS som tilleggsbeskyttelse.
- Når oppkoblingen er gjort, skal informasjonssikkerheten ved bruk være på lik linje som om man var innenfor virksomhetens egne lokaler.Hjemmevakt-pc skal ha god virusbeskyttelse og rutiner for oppdatering av virusdefinisjonene og -programmet etter leverandørens anbefalinger.
- Ethvert brudd på sikkerhetsrutinene skal logges og undersøkes særskilt med hensyn til om sikkerhetsrutinene er gode nok eller bør endres.
- Hjemmevakt-pc skal ha passordbeskyttet kryptert harddisk for å hindre tilgang fra uvedkommende dersom maskinen blir stjålet, mistes eller lignende. Alternativt skal den låses inn, for eksempel i et stålskap, når den ikke er i bruk.

For klasse 2 driftskontrollsystem gjelder følgende;

- Det skal være utarbeidet en egen risiko- og sårbarhetsanalyse for oppkobling fra hjemmevakt-pc.
- Basert på risikoanalysen skal det utarbeides sikkerhetsrutiner for oppkobling fra hjemmevakt-pc. Oppkobling med hjemmevakt-pc skal bare skje dersom det er absolutt behov for det.
- Oppkobling fra hjemmevakt skal kun skje etter tillatelse i hvert enkelt tilfelle. Oppkoblingen skal logges.
- IKT-driftspersonell skal ikke ha selvstendig tilgang til funksjoner for administrasjon av sikkerhet og systemrettigheter. Dette tilsvarer tilgang som systemadministrator eller driftsoperatør på driftskontrollsystemet. Dersom slik tilgang er nødvendig for sikring og/eller gjenoppretting av normal drift, skal tilgangen autoriseres i hvert enkelt tilfelle.
- Oppkobling mot driftskontrollsystemet skal skje via sikker kanal gjennom brannmur for kommunikasjon, for eksempel VPN. Sikring av kommunikasjonen skal også omfatte eventuelt trådløst nettverk.
- Utstyr for hjemmevakt-pc skal være dedikerte for denne type bruk. Det er ikke tillatt å benytte hjemmevakt-pc for andre formål, som for eksempel lokal bruk av internett eller e-post. Slik bruk skal kun skje via sikret kommunikasjonskanal og ha sikker bruk på lik linje som når tilkobling skjer innenfor virksomhetens egne lokaler.
- Hjemmevakt-pc skal ha god virusbeskyttelse og rutiner for oppdatering av virusdefinisjonene og -programmet etter leverandørens anbefalinger.
- Hjemmevakt-pc skal ha passordbeskyttet kryptert harddisk for å hindre tilgang fra uvedkommende dersom maskinen blir stjålet, mistes eller lignende. Alternativt skal den låses inn, for eksempel i et stålskap, når den ikke er i bruk.

For klasse 1 driftskontrollsystem gjelder følgende;

- Det skal være utarbeidet en egen risiko- og sårbarhetsanalyse for oppkobling fra hjemmevakt-pc. Sikkerhetsrutinene som skal utarbeides for hjemmevaktbruk skal blant annet baseres på denne.
- Oppkobling mot driftskontrollsystemet med hjemmevakt-pc skal bare skje dersom det er absolutt behov for det og skal vurderes særskilt i hvert enkelt tilfelle.
- Kommunikasjonen mellom hjemmevakt-pc og driftskontrollsystem skal være sikret i form av sikker pålogging med bruk av passord. Dette skal også gjelde for eventuell bruk av trådløst nettverk.
- Hjemmevakt-pc skal ha god virusbeskyttelse og rutiner for oppdatering av **virusdefinisjonene og -programmet etter leverandørens anbefalinger.**

Ekstern kvalitetssikring av sikkerhetsrutiner og – krav

Systemsikkerhet rundt ekstern oppkobling er komplisert og svært spesialisert. Feilkonfigureringer og rutiner/prosedyrer som ikke samsvarer med kravene øker risikoen for uønskede hendelser i driftskontrollsystemet. Det anbefales derfor at virksomhetene foretar en ekstern kvalitetssikring av de rutinene og kravene som etableres rundt fjerntilgang spesielt og informasjonssikkerhet generelt. Dette er også viktig i forhold til å øke kompetansen for dette i egen virksomhet da man får tilgang til eksperter på området.

Fjerntilgang fra leverandør

Fjerntilgang fra leverandør skal vurderes restriktivt og være under særlig god kontroll hos enheten. For driftssentraler i alle klasser gjelder følgende:

- Det skal være utarbeidet en egen risiko- og sårbarhetsanalyse for oppkobling fra leverandør.
- En egen sikkerhetsinstruks for oppkobling fra leverandør skal utarbeides.
- Oppkobling mot driftskontrollsystemet skal skje via sikker kanal gjennom brannmur for kommunikasjon, for eksempel VPN. Sikring av kommunikasjonen skal også omfatte eventuelt trådløst nettverk. For klasse 3-anlegg kreves i tillegg to-nivå autentisering med bruk av engangspassord eller tilsvarende sikkerhet.
- Terminering av oppkobling skal kunne skje fra driftsentralen.
- Det tillates ikke fjerntilgang mot utstyr når driftssentralen er ubemannet.
- Leverandører skal normalt ikke ha selvstendig tilgang til funksjoner for administrasjon av sikkerhet og systemrettigheter. Dette tilsvarer tilgang som systemadministrator eller driftsoperatør på driftskontrollsystemet. Dersom slik tilgang er nødvendig for sikring og/eller gjenoppretting av normal drift, skal tilgangen autoriseres i hvert enkelt tilfelle.
- Tilgang skal i hvert enkelt tilfelle:
  - være forhåndsavtalt og varslet
  - spesifikt tillates av enheten
  - være tidsbegrenset
- Det skal inngås særskilte sikkerhetsavtaler mellom enheten og leverandørene der alle krav enheten har til sikkerhetstiltak og rutiner hos leverandør skal inngå. Leverandørens tiltak skal dokumenteres.

Eksempel på løsning for fjerntilgang til driftskontrollsystemet for leverandør:

Oppkall, forhåndsvarsling og godkjenning av tilgang, hemmelig nummer/adresser

”Tilbakeringing", kontroll, autentisering eller liknende

Innlogging, passord

Avslutning, automatisk utlogging etter en viss tid

Særskilt om tilgang utenfor adgangskontrollert sone

For hjemmevakt med tilgang til driftskontrollsystemet (driftsoperatør, IKT-drift eller leverandørstøtte) der bruk av tilgang tillates utenfor etablert adgangskontrollert sone, skal man være svært restriktive med å tillate oppkobling mot driftskontrollsystemet. Det kreves særskilte tiltak for å oppnå tilsvarende beskyttelse av utstyr for tilgang. Med ”utenfor adgangskontrollert sone” menes utenfor enhetens lokaler eller hjemmet til personen(e) som har hjemmevakt. Formålet er primært å sikre at ikke utstyr og system kan misbrukes eller ødelegges av uvedkommende, enten ved innbrudd, tyveri eller annen form for urettmessig overtakelse. Kravet må tillempes hva som er praktisk, men må minst omfatte følgende tiltak og gjelder driftskontrollsystem i alle klasser:

- Det skal utarbeides egen sikkerhetsinstruks for denne type oppkobling.
- Oppkobling når driftskontrollrommet er ubemannet er ikke tillatt.
- Utstyr for tilgang (hjemmevakt-PC) skal hele tiden være under opppsyn - særlig ved transport (i bil/på reise mv).
- Utstyret skal ikke lånes ut til uautoriserte personer.
- All bruk med pålogget utstyr tillates kun dersom forholdene tillater det ut i fra kravene i § 6-2 om ”Beskyttelse av informasjon”.
- Dersom personen som skal koble seg opp mot driftskontrollsystemet befinner seg på et offentlig sted, skal man være ekstra restriktive med tillatelse til oppkobling. Sikkerhetsinstruksen skal omhandle dette spesielt. Bruker må autentiseres ved pålogging for å bruke utstyret.
- All bruk av utstyret skal registreres/logges på sikker måte.
- Hjemmevakt-pc skal ha kryptert harddisk for å hindre tilgang fra uvedkommende dersom maskinen blir stjålet, mistes eller lignende. Alternativt skal maskinen låses inn, for eksempel i stålskap, når den ikke er i bruk og ikke innenfor enhetens lokaler.

Revidering av risikovurderinger

For alle ordninger der tilgang fra hjemmevakt og fjerntilgang fra leverandør tillates, skal enheten minimum 2 ganger årlig foreta en oppdatering av sine risikovurderinger knyttet til dette. Slik vurdering skal også foretas ved sikkerhetsbrudd eller ved endringer (av organisasjon, prosedyrer og teknologi) i eller i tilknytning til driftskontrollsystemet eller andre systemer som er relevante for slik tilgang

6.4.2.12 Programfeil-/svakheter og bakdører

De fleste programmer har sikkerhetsmessige svakheter i større eller mindre grad. Det forekommer også at leverandører eller deres programutviklere mer eller mindre bevisst lager forenklede og ofte skjulte/udokumenterte tilgangsveier inn i programmet/systemet, såkalte ”bakdører”. Dette gjør de for at de selv på en enkel måte kan oppdatere og feilrette programmer og informasjon. Ovennevnte svakheter og skjulte tilgangsveier kan forårsake utilsiktede feilfunksjoner eller utnyttes av andre til hacking (datainnbrudd) eller spredning av ondsinnet program. Enheten:

- Må stille krav til leverandører gjennom skriftlige avtaler om at det er uakseptabelt med tilsiktede sikkerhetshull for viktig programvare som leveres til kraftforsyningen
- Må stille krav til årvåkenhet og sikkerhetspolicy hos de ansvarlige hos alle parter
- Må gjennomføre en systematisk oppfølging og implementering av sikkerhetsoppdateringer/nye versjoner etter hvert som feil og svakheter oppdages
- Må kreve at leverandører gjennomfører tilsvarende systematiske oppfølginger og implementeringer av sikkerhetsoppdateringer/nye versjoner

Husk at oppdateringer av programvare og utstyrskonfigurasjon som ikke omfatter sikkerhetsfunksjoner kan introdusere feil for både funksjoner og systemkonfigurasjon, i form av utilgjengelighet for viktige ressurser både ved og som en følge av oppdateringen. Oppdatering av for eksempel sambandsutstyr som rutere og svitsjer kan få alvorlige følger for driftskontrollfunksjonen. Slike oppdateringer bør derfor være grundig testet på forhånd.

Konfigurasjonskontroll og liknende

Det er nødvendig til enhver tid å ha sikkerhetsmessig konfigurasjonskontroll over systemet. Alle endringer skal planlegges, evalueres i forhold til sikkerhet og dokumenteres. Kravene til konfigurasjonskontroll skal være beskrevet og ivaretatt i IT-sikkerhetsinstruks og skal omfatte både maskinvare, programvare, nettverksarkitektur og brukere. Særlig må enheten være oppmerksom på:

- Endringer/oppdateringer av operativsystem og annen programvare.
- Tilkobling av eksterne forbindelser.
- Innføring og utfasing av lagringsmedier.

For tilgangssystemer (for eksempel tilgangskontrollsystemer og brannmur) anbefales evaluerte og sikkerhetssertifiserte systemer og utstyr, se § 6-2 Beskyttelse av informasjon.

6.4.2.13 Kontroll med ondsinnet programvare

Spredning av ondsinnet programvare er en risiko med høy sannsynlighet og med betydelige konsekvenser. Ondsinnet programvare omfatter virus, ormer, trojanske hester, logiske bomber, samt andre uvedkommende program som kan skade, hindre eller eksponere enheten for uvedkommende.

Kontroll med ondsinnet programvare skal være en helt selvfølgelig del av den generelle IT-sikkerheten. Det er svært viktig at driftskontrollsystemet beskyttes mot denne type trusler. Det er fullt mulig å infisere driftskontrollsystemet ved bruk av løse minnepinner/harddisker eller tilkobling av bærbare datamaskiner som har vært utenom eget sikkerhetsdomene.

Brannmuren bidrar, men ideelt sett bør driftskontrollsystemet ha automatisk viruskontroll. Likevel bør slik beskyttelse etableres i nært samråd med leverandør. Viruskontrollprogrammer søker ofte etter oppdateringer via internett. Dette kan i seg selv eksponere driftskontrollsystemet for trusler og redusere funksjonaliteten, og i verste fall infisere driftskontrollsystemet. Samråd med leverandørene kan gi optimal beskyttelse av driftskontrollsystemet samtidig som full funksjonalitet ivaretas.

De farligste angrep kommer imidlertid fra latente virus som utnytter ukjente svakheter og som spres før mottiltak er utviklet og distribuert. Denne type virus er det vanskelig å beskytte seg mot. Den beste beskyttelsen er at enhetene har streng tilgangskontroll, men også at enhetene har gode varslingsrutiner med leverandørene. Leverandørene blir gjerne gjort oppmerksomme på denne type trusler tidlig, og da er det viktig at enhetene i samarbeid med sin leverandør raskt får satt i gang tiltak for å detektere og fjerne trusselen, eventuelt få iverksatt andre beredskapstiltak før viruset aktiveres.

6.4.2.14 Henvisninger

Internasjonalt finnes flere kilder til informasjon om trusler/sårbarheter, spesielle forhold og aktuelle tiltak for tilgangskontroll i driftskontrollsystemer (SCADA/ Industrial Control Systems - ICS).

National Institute of Standards and Technology (NIST):

SP 800-82 Guide to Industrial Control Systems (ICS) Security

SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations

(appendix I: Industrial Control Systems (ICS) Security)

Se mer på http://csrc.nist.gov

United States Computer Emergency Readiness Team (US-CERT):

Mange referanser til relevante standarder / rapporter finnes hos US-CERT:

http://www.us-cert.gov

United Kingdom National Centre for the Protection of National Infrastructure (CPNI))

Process Control and SCADA Security (framework + 7 spesialtemaguider)

Good Practice Guide on Firewall Deployment for SCADA and Process Control Network

Se http://www.cpni.gov.uk

6.4.3 Systemsikkerhet

Systemsikkerhet oppnås ved en optimal kombinasjon av redundans og beskyttelse. Avhengig av hva slags hendelser og handlinger som inntreffer, er disse dels alternativer, og dels utfyller de hverandre. I tillegg kommer blant annet forebyggende sikkerhet og evne til å kunne gjenopprette funksjon. Forskriften angir her krav til redundans for driftskontrollsystemer i ulike klasser. Krav til gjenoppretting, beskyttelse og forebyggende sikkerhet er beskrevet i andre deler av forskriften, se §§ 5-5 Sikringsnivå, 4-5 Adgangskontroll, 3-5 Gjenoppretting av funksjon, og 6-4 b Tilgangskontroll.

Bestemmelsen setter ikke krav til driftskontrollsystemer i klasse 1. Enheter som benytter driftskontrollsystem i klasse 1 anbefales å vurdere behovet for systemsikkerhet ut fra lokale forhold, i henhold til §§ 5-4 analyse og 5.5 sikringsnivå. Det skal minimum være ett talesamband til alle klassifiserte anlegg som er tilknyttet driftskontrollsystemer i denne klassen. Nærmere veiledning for klasse 2 og 3 omtales i vedlegget til denne veiledningen.

6.4.3.1 Redundans

Ingen enkeltfeil eller hendelse skal kunne sette driftskontrollsystemet eller viktige funksjoner ut av drift. Driftskontrollsystemer med tilhørende hjelpesystemer og andre viktige elementer skal, avhengig av klasse, derfor bygges som redundante systemer etter N-1 kriteriet. Det betyr at dersom feil eller hendelse setter et system ut av spill, skal et annet system overta viktige funksjoner. Tilstrekkelig redundans må bygges inn i systemet ved dublering og separering, slik at det opprettes reell uavhengighet. Separering kan utføres ved tilstrekkelig fysisk avstand eller fysisk atskillelse, eksempelvis branncelle.

Redundans kan oppnås på følgende prinsipielle metoder:

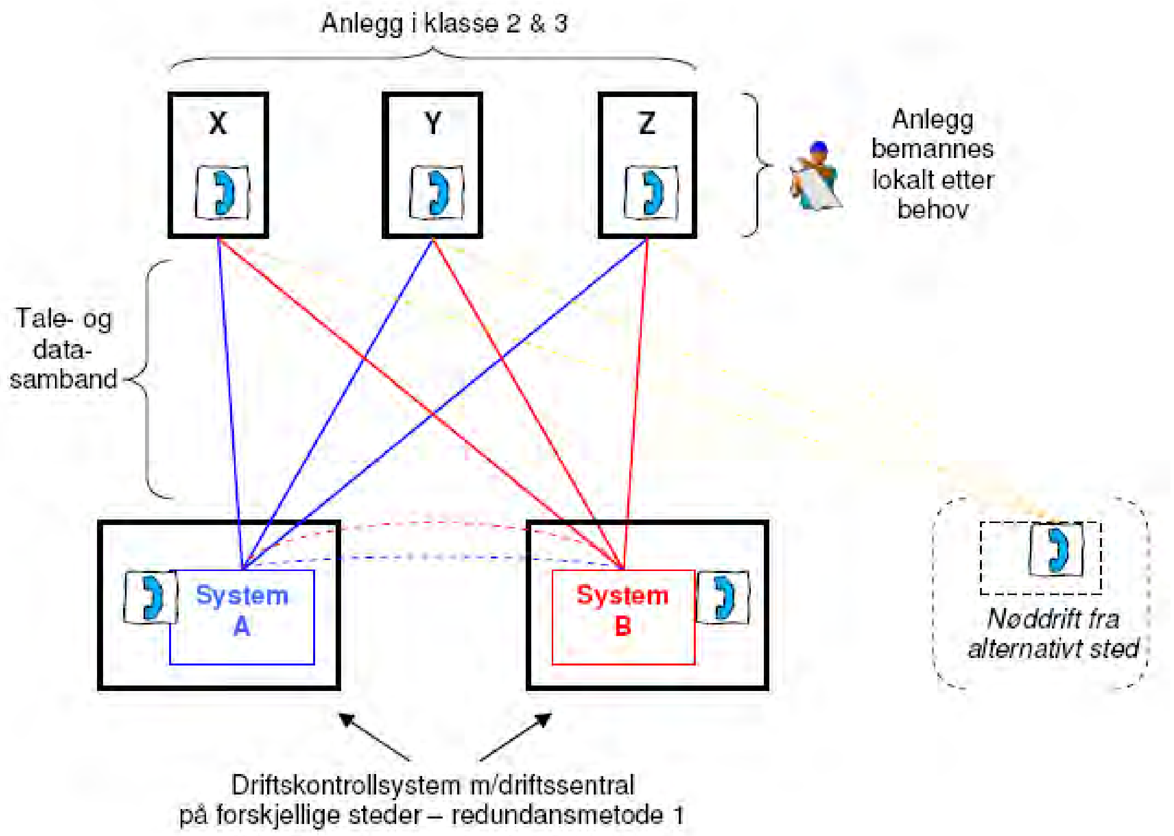
- Metode 1: Dublering og separering på alternativt sted, med tilstrekkelig fysisk avstand. Eksempel: Den andre prosessmaskinen, med tilhørende nødvendig utstyr som sambandskomponenter, nødstrøm og kjøling, er plassert i et annet bygg.
- Metode 2: Dublering og separering på samme sted. Eksempel: Begge prosessmaskiner i hver sin branncelle i samme bygg.
- Metode 3: I noen tilfeller kan lokalstyring i kraftforsyningsanlegg godkjennes som redundans. Det forutsetter lokal kontrollutrustning, samt tilstrekkelig bemanning og kompetanse.
- ”Fallback” i form av ulike alternativer og reserveløsninger eller i ulike kombinasjoner av disse metodene.

Metode 1 til 3 representerer likeverdig/symmetrisk redundans, det vil si at alle vesentlige funksjoner ivaretas tilnærmet fullt ut. ”Fallback” gir asymmetrisk redundans. Det vil si at kun de viktigste funksjoner ivaretas på et minimumsnivå, slik at noe fungerer på tross av det inntrufne.

For klasse 2 og 3 vil for eksempel ”fallback” være nødvendig, men ikke tilstrekkelig. Et viktig moment er også å vurdere redundansløsninger i forhold til bemanning, spesielt ved hendelser der mannskapsevakuering kan inntreffe, for eksempel pålagt evakuering ved brann. Selv om systemteknisk funksjon er intakt grunnet redundans, kan evakuering gjøre systemet utilgjengelig for driftsfunksjonen. Dette er spesielt viktig å vurdere ved bruk av redundansmetode 2, plassering i samme bygg.

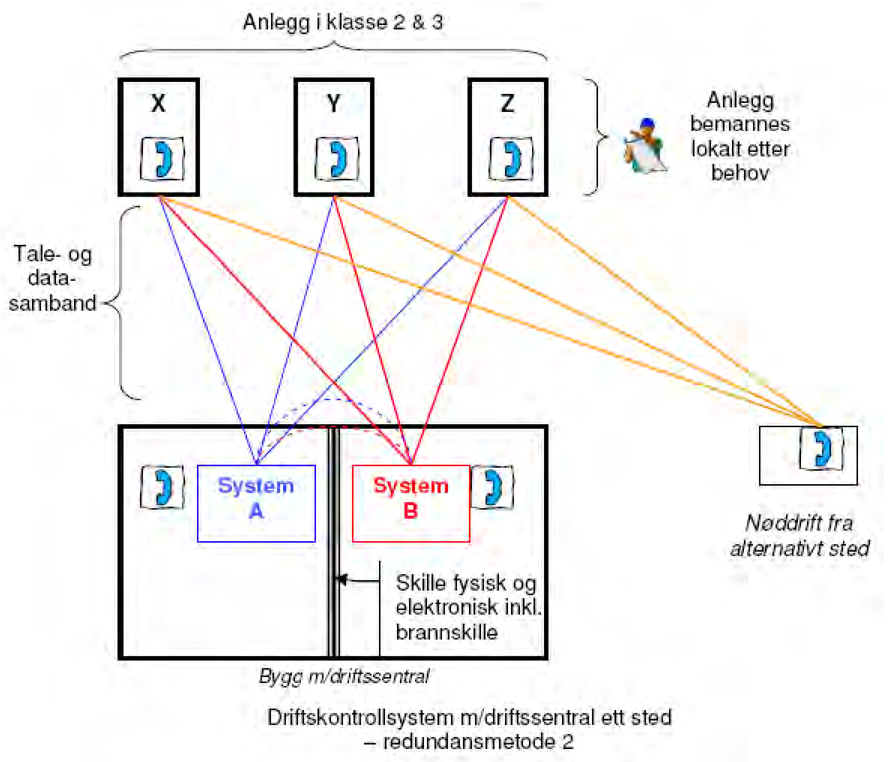
De følgende figurene illustrerer prinsippene for de ulike metodene 1 til 3. Stiplede deler av figurene indikerer opsjoner som tillegg til metodens redundans.

Samband mellom de symmetriske delsystemene i A og B vil gi fleksibilitet ved feil, slik at de ulike systemene kan ha størst mulig grad av redundans inntil gjenoppretting er fullført. Dette kan kombineres med nødvendig synkronisering mellom A og B.



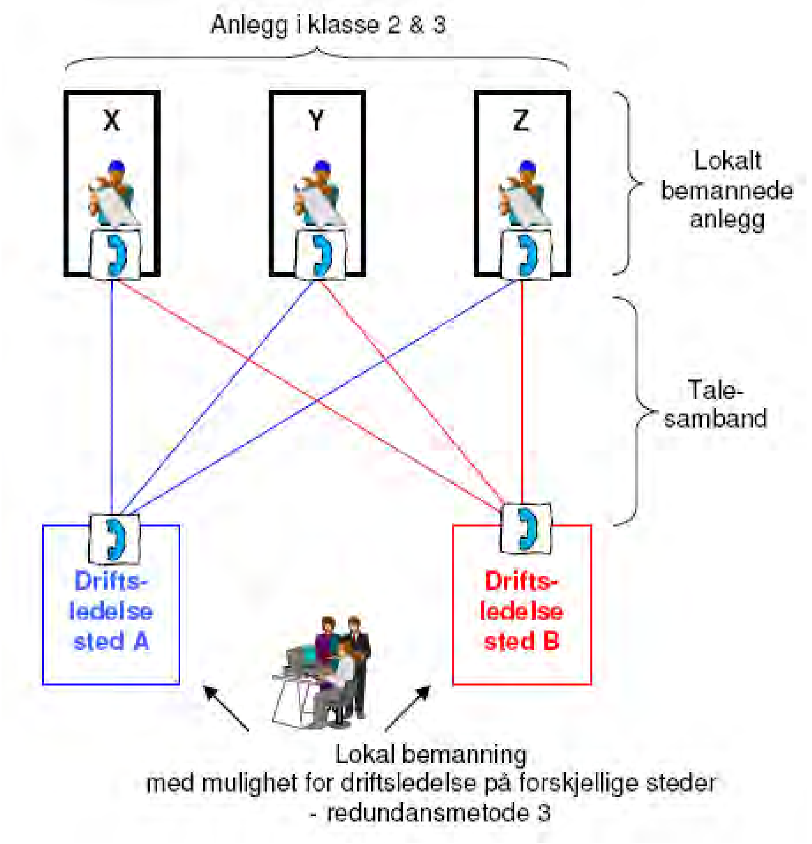
Figur 4: Redundansmetode 1

For redundansmetode 1 vil nøddrift kunne kombineres med A eller B, eller gi økt driftssikkerhet ved etablering fra annet sted.



Figur 5: Redundansmetode 2

For redundansmetode 2 er nøddrift på alternativt sted i utgangspunktet et krav for klasse 2 og 3 driftskontrollsystem, med hensyn til risiko for evakuering. Dette inkluderer også separate talesamband for lokalstyring fra alternativt sted til det enkelte anlegg for å tilfredsstille krav om dublerte samband klasse 2 og 3 anlegg.



Figur 6: Redundansmetode 3

For redundansmetoder (type 2 og 3) der redundant systemløsning for driftskontroll baseres på styring med lokal bemanning, vil kravene til bemanning være gitt av behov for styring og oppdatert driftsstatus for det enkelte anlegg. Det skal i en slik løsning alltid være tilgjengelig lokal bemanning for nødvendig styring, overvåkning og innhenting av driftsstatus. Dette innebærer at iverksettelse av lokalstyring og organisering av bemanning i klasse 2 og 3 anlegg må være i henhold til krav om at den enkelte redundante løsning for driftskontroll på kort varsel skal overta ved feil. I slike tilfeller vil dette måtte være en del av ordinær driftsplan for driftskontrollsystemet som raskt skal kunne iverksettes.

Lokalstyring med bemanning og nødvendig samband (se alternativ driftsløsning nedenfor) vil komme i tillegg til dette som en del av beredskapsplan for å håndtere ekstraordinære hendelser, uansett redundansmetode.

6.4.3.2 Beskyttelse

Det skal ikke bare tas hensyn til enkeltfeil, men også systematiske feil, hendelser og tilsiktede handlinger. For eksempel kan uvær av en viss styrke rive ned begge sambandsveier om begge er dårlig beskyttet/svakt dimensjonert. EMP/EMI kan ødelegge begge prosessmaskiner eller kommunikasjonsutstyr om ikke disse er beskyttet, eller samme/simultane feil i programvare eller maskinvare kan sette begge delsystemene ut av drift samtidig. Redundans gir med andre ord ikke svar på alle utfordringer/risikoer.

Ulike former for beskyttelse må også vurderes og gjennomføres. Det må vurderes om en skal dublere likt med likt for å ha driftstekniske fordeler (reservedeler og liknende), eller å dublere med ulikt, for eksempel ulike typer servere/rutere, ulike typer sambandsveier eller annen leverandør. Dersom en dublerer likt med likt, må en nøye planlegge ”fallback” i tilfelle systematiske/simultane feil.

Det må også planlegges med en overlevelsesevne i ekstraordinære og særlig dramatiske situasjoner. Dette innebærer blant annet at den enkelte komponent/det enkelte delsystem gis tilfredsstillende beskyttelse (fysisk og elektronisk). Krav og anbefalinger til elektronisk beskyttelse, etter denne paragrafens pkt. b Tilgangskontroll.

For et redundant system må en også vurdere beskyttelsesnivå og omfang på alle de alternative mulighetene for driftskontroll i en samlet risiko- og sårbarhetsvurdering, balansering og hensiktsmessighet.

Fysisk sikkerhet

Krav til fysiske sikringstiltak for driftskontrollsystemer, se § 5-5 Sikringsnivå.

Nødstrøm

Krav til nødstrøm for driftskontrollsystemer, se § 5-5 Sikringsnivå.

6.4.3.3 Alternativ driftsløsning

Enheten må i tillegg ha alternative driftsløsninger for å kunne håndtere situasjoner med svikt i de redundante systemene. Driftsløsningen må minst omfatte samband, nødstrøm og kompetanse, hvorav kun de viktigste funksjonene blir ivaretatt på et minimumsnivå. Dette er også kalt ”fallback” og må sees i sammenheng med tiltak i beredskapsplan, § 5-5 Sikringsnivå, og § 6-5 Mobile radionett – driftsradio.

Eksempler på alternativ driftsløsning (”fallback”):

Reservesystemløsning omfatter bare de mest vitale systemkomponenter for drift av primærfunksjoner i kraftforsyning og nett. Andre funksjoner må ivaretas manuelt eller på annen måte

Ved feil i driftssentralens kontrollanlegg, vil alternativ driftsløsning for eksempel være å gå tilbake til manuelle rutiner og papirdokumentasjon. Kraftforsyningsanleggene kan styres med lokal bemanning, og samband med driftssentralen baseres på talesamband eller ordonnans.

6.4.3.4 Gjenopprettingsevne

Gjenopprettingsevnen til en driftssentral skal følge prinsippene i § 5-5 Sikringsnivå, hvorav funksjonen til klasse 3 anlegg skal gjenopprettes raskt, og funksjonen til klasse 2 anlegg skal gjenopprettes innen rimelig tid. Dersom et redundant delsystem svikter, forsvinner også redundansen. Ved en eventuell ny feil vil driftskontrollfunksjonen kunne reduseres eller forsvinne helt. Det forutsettes derfor at man straks, eller så fort forholdene tillater dette, reparerer og setter det (del-)systemet som ble skadet eller liknende i driftsklar stand.

Krav til reparasjonsberedskap for driftskontrollsystemer, se § 3-5 Gjenoppretting av funksjon.

6.4.3.5 Uavhengighet av offentlige nett og teletjenester

Driftskontrollsystemer i klasse 3 skal kunne fungere uavhengig av offentlige nett og teletjenester. Med ”offentlige nett og teletjenester” menes nett for tilgang til offentlig elektronisk kommunikasjonstjeneste og de tjenestene som tilbyder av offentlige elektroniske kommunikasjonstjenester gir tilgang til (se Lov om elektronisk kommunikasjon).

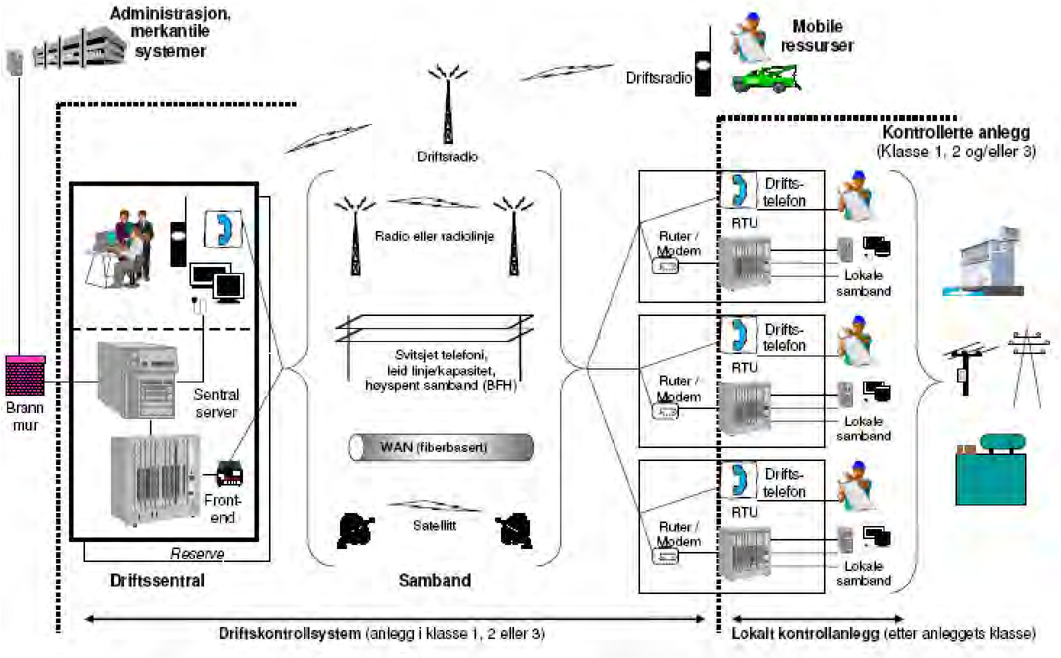
Dette er nett og tjenester der tilgang tilbys til allmennheten og virksomheter i et kommersielt marked for elektronisk kommunikasjon. Det omfatter mange ulike tjenester (bredbånd, fast- og mobiltelefoni), herunder også såkalt overføringskapasitet.

6.4.3.6 Samband og sambandsveier som inngår i driftskontrollsystemet

Driftskontrollsystemets samband omfatter alle samband som fører signaler for data og tale mellom driftssentral og kraftforsyningsanleggene som styres, men ikke lokalt inne i selve kraftforsyningsanlegget. Det vil si sambandsveiene fra driftssentralens front-end kommunikasjonsgrensesnitt til grensesnittet med kraftverkets ytre sambandskode (sender/mottaker enhet), ofte kalt RTU (Remote Terminal Unit). Øvrig kontrollsystem fra RTU og innover til lokalstyring er en del av kraftverket, og kravene her følger kraftverkets klasse. Dette er illustrert i figur på neste side. Merk likevel at dersom en del av et kraftverks samband fører signaler videre til andre kraftverk (ringforbindelse eller radial), vil dette sambandet inngå i driftskontrollsystemet. Tilsvarende gjelder også dersom lokalt utstyr for nødstrøm er nødvendig for drift av slike samband.

Sambandsvei er den vei signaler med informasjon (tale og data) formidles via radiokanal (driftsradio, satellitt, mobiltelefonnett) og/eller kabel (kobber, optisk fiber) mellom to endepunkter for elektronisk kommunikasjon. I sambandsvei inngår også utstyr som formidler signalene (transmisjons- og koplingsutstyr) til/mellom transmisjonsmediene som benyttes.

Ved krav om fysisk separasjon av sambandsveier gjelder dette både utstyr og fysiske transmisjonssystemer som inngår i hver sambandsvei.



Figur 7: Skisse av skille mellom driftskontrollsystem og lokalt kontrollanlegg

6.4.3.7 Systemsikkerhetskrav i driftskontrollsystemer etter klasse

For systemsikkerhetskrav i driftskontrollsystemer etter klasse vises det til vedlegg til denne veiledningen. Vedlegget er underlagt taushetsplikt etter beredskapsforskriften § 6-2 og unntatt offentlighet etter offentleglova § 13 første ledd.

Stamnett

Det fremgår også av beredskapsforskriften at enheter med driftskontrollsystem i klasse 3 skal ha, og dermed har ansvaret for å etablere, redundante forbindelser til andre relevante driftskontrollsystemer i klasse 2 og 3. Med utgangspunkt i dette kravet er det dermed et mål at alle vesentlige driftskontrollsystemer (klasse 3 og 2) i landet settes sammen til et redundant helhetlig system med fysisk og elektronisk uavhengige kommunikasjonsveier.

Statnett har i praksis det overordnete ansvar for det kommunikasjonsmessige stamnettet (landsentral og regionsentraler) og ut til de andre enhetene i sentral og regionalnettet. Disse skal på sin side sørge for å medvirke til, og om nødvendig ta initiativ til nevnte etablering.

6.4.4 EMP- og EMI-beskyttelse

Driftskontrollsystemer i klasse 2 og 3 skal beskyttes mot all elektromagnetisk støy og alle typer radiobølger som kan ødelegge utstyret eller påvirke dets funksjonsdyktighet og pålitelighet. Tiltak må i noen grad avpasses etter stedlig risiko, samt anleggets betydning og egenskaper.

Kort beskrevet kan EMI og EMP forklares slik:

- Elektromagnetisk interferens (EMI) er elektromagnetiske signaler som kan forstyrre for eksempel samband eller IKT-utstyr. Eksempler på EMI er radiostøy fra en elektromotor eller jammesignaler som blokkerer radiotrafikk.
- Elektromagnetisk puls (EMP) er en radiofrekvent meget kortvarig energipuls med meget stor energitetthet, som medfører fysiske ødeleggelser i utstyret som rammes. Dette er en svært kraftig utgave av EMI, som kan forårsakes av lynutladninger, kjernevåpeneksplosjoner eller mikrobølgevåpen.

Elektromagnetisk puls (EMP) og elektromagnetisk interferens (EMI) er elektromagnetisk stråling sammensatt av elektrisk felt og magnetisk felt. Slik stråling kan ødelegge utstyr som inneholder elektronikk. Denne typen stråling kan også ha effekt på personell, men da i vesentlig høyere strålingsstyrker. Forskriftens bestemmelser gjelder effekter av slik stråling på elektronikk og beskyttelse beregnet på teknisk utstyr som inngår i driftskontrollsystemet.

6.4.4.1 Vurdering og beskyttelse mot EMP og EMI

Her henvises det til vedlegg til denne forskrift, underlagt taushetsplikt etter beredskapsforskriften § 6-2 Beskyttelse av informasjon og unntatt offentlighet etter offentleglova § 13 første ledd.

6.4.5 Brannsikkerhet

For brannsikkerhet i driftsentraler se punkt 5.5.3 Brannsikkerhet

6.4.6 Beredskapsrom

For driftssentraler i klasse 2 og 1 vil behovet for beredskapsrom bli vurdert av NVE.

Beredskapsrommet skal tjene som nøddriftssentral, ved for eksempel ødeleggelse eller havari i den ordinære driftssentralen. Beredskapsrommet skal gi beskyttelse mot hendelser som krever fysisk beskyttelse og sikre viktige funksjoner. Reserveløsningen av et redundant system kan lokaliseres i beredskapsrommet. Dersom beredskapsrommet benyttes til daglig, må det sikres etter kravene som funksjonen tilsier. Beredskapsrommet skal kunne være operativt på kort varsel. Enheten må derfor:

- Gjøre forberedelser for enkel flytting og tilkobling av sambands- og datautstyr fra den ordinære driftssentralen.
- Ha oppdaterte utstyrslister og plan for utstyr som skal bli tilført fra andre steder.
- Sørge for sambandsveier, nødstrøm og øvrig nødvendig utstyr.
- På kort varsel kunne utstyre beredskapsrommet med de hjelpemidler (oppdaterte kart, oversikter, sambandsutstyr og annet), som er nødvendig for å:
  - kunne lede den del av kraftforsyningen selskapet er ansvarlig for.
  - ha løpende forbindelse med høyere og lavere ledd innen KBO.
  - kommunisere med øvrige relevante etater (politi, fylkesmenn og andre).

6.4.6.1 Prosjektering

Ved prosjektering av beredskapsrom benyttes kravene til tilfluktsrom etter forskrift om tilfluktsrom, FOR-1995-03-15-254. I tillegg skal kravene i etterfølgende tabell være oppfylt.

Plassbehov	Gassluse	Ventilasjon
Min. 2 m2/person.	I alle beredskapsrom. Innvendige mål minimum: L x B = 2,5 x 1,5 m	Normalventilasjon: Min. 20 m3/h/pers. Filterventilasjon: Min. 10 m3/h/pers.

Nødstrømsforsyning med batterier eller dieselaggregat vurderes i hvert enkelte tilfelle, se kravene til nødstrøm for driftssentral § 5-5 Sikringsnivå. Enheten må foreta sluttkontroll av tetthet, overtrykk, installasjon og andre relevante forhold.

Det skal foreligge oppdaterte utstyrslister, og planer for utstyr som skal bli tilført. For utstyrsliste, se vedlegg.

6.4.6.2 Drift og vedlikehold

Det skal være utpekt personer som er ansvarlige for drift og vedlikehold av beredskapsrom.

Den som er ansvarlig for vedlikehold av beredskapsrom skal ved regelmessige inspeksjoner sørge for at rommets 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. 15o C og den relative fuktigheten ikke over 50 - 60 %.

Beredskapsrom 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 for liste over hva som skal kontrolleres ved de rutinemessige inspeksjonene.

6.4.6.3 Kontroll

I tillegg til forannevnte inspeksjoner skal alle beredskapsrom kontrolleres minimum en 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 for sjekkliste for disse kontrollene.

§6-5 Mobile radionett - driftsradio

Alle enheter i KBO som er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon skal ha tilgang til et mobilt sambandssystem.

Dette sambandssystemet skal:

a) Ha tilstrekkelig dekningsgrad for kraftforsyningens anlegg og drift,

b) fungere uavhengig av funksjonssvikt i offentlige nett,

c) ha tilstrekkelig nødstrøm ved omfattende eller langvarige strømbrudd,

d) ha nødvendig funksjonalitet med blant annet direkte apparat til apparat kommunikasjon, gruppesending og felles oppkall, og

e) kunne fungere som reservesamband om annet samband svikter.

Veiledning

De fleste enhetene i KBO er i større eller mindre grad avhengige av mobilt samband (driftsradio, også kalt ”lukket nett” eller PMR – ”Private Mobile Radio”). Dette gjelder både administrativt og i den operative driften, som for eksempel ved arbeider i kraftsystemet, utrykninger i ekstraordinære situasjoner og gjenoppretting av funksjon. Av hensyn til drifts- og reparasjonsberedskapen og på grunn av personsikkerheten skal man ha tilgang til mobilt samband med høy tilgjengelighet og med god dekningsgrad. Bestemmelsen stiller derfor funksjonelle og sikkerhetsmessige krav til slikt samband, som dagens tilgjengelige systemer for offentlige mobiltelefontjenester IKKE gir.

6.5.1 Funksjon uavhengig av andre sambandsløsninger

For å sikre funksjon uavhengig av funksjonssvikt i offentlige nett, samt reservefunksjon ved svikt i annet samband, er det nødvendig med fysiske sikringstiltak for driftsradiostasjoner:

- Viktige og utsatte stasjoner bør vurderes bygget i betonghytte, eventuelt stålcontainer (dette gir bl.a. beskyttelse mot brann, innbrudd og hærverk).
- Viktige komponenter bør plasseres i avlåste telerom uten vinduer, med innbruddsalarm til døgnbemannet sentral (eventuelt hjemmevakt).
- Vinduer bør tildekkes med solide lemmer, låst eller boltet til innside
- Kabelføringer til mast bør føres i tildekket kanal eller i kabelbro utenfor rekkevidde.
- 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 reserveveier.
- Master bør beskyttes med klatrehinder.
- Alle rom som inneholder elektronisk utstyr som har betydning for driften av driftsradiostasjonen (telerom og liknende) skal gjennom ROS-analyse vurderes skjermet mot EMP/EMI, etter § 6-4 Særlige krav til driftskontrollsystemer, punkt d.

6.5.2 Nødstrøm

Sikring av strømforsyning er naturlig delt mellom utendørs- og innendørsanlegg. Dette avsnittet tar i hovedsak hensyn til små stasjoner som huser en eller flere basestasjoner, samt kontrollutstyr i driftsradionett. Der utstyr er plassert i større stasjoner, som f.eks. radiolinjestasjoner, er nødstrøm ivaretatt gjennom kravene til radiolinjestasjonen.

Ordinær strømforsyning, nødstrøm og samband bør føres inn i bygninger gjennom jordkabler. Stasjonens kabling bør organiseres med hensyn til beskyttelse mot overspenninger. Sikringsskap og liknende plasseres innendørs. Likerettere bør dupliseres og overvåkes med alarmer.

Stasjonene bør utstyres med batterianlegg med driftstid minst 72 timer. Alternativt kan stasjonen ha batterianlegg med driftstid minst 48 timer dersom stasjonært nødstrømaggregat er installert. Krav til nødstrøm kan reduseres dersom god fysisk tilgjengelighet i alle situasjoner med utfall av ordinær strømforsyning kan dokumenteres.

Dersom radiosystemet er avhengig av for eksempel signaloverføring og sentrale funksjoner, må alle nødvendige deler av systemet oppfylle tilsvarende krav som for radiostasjonene. I viktige dekningsområder bør det være minst to overføringsmuligheter (redundans).

6.5.3 Reservedeler og reparasjonsberedskap

Enheten bør inkludere reparasjon av driftsradioanlegg i sin beredskapsplan, og ha et relevant lager av de mest utsatte komponentene i radiosystemet. Der det benyttes viktige enheter med svært lang leveringstid, bør leverandøren kontaktes for å inngå avtale om lagerhold. Egne medarbeidere bør ha tilstrekkelig kompetanse for feilretting. Ved behov for assistanse, avtales dette med leverandør eller andre med tilstrekkelige kvalifikasjoner.

For krav til nødvendig kompetanse for installasjon av utstyr i radioanlegg vises det til Lov om elektrisk kommunikasjon (ekomloven) § 2-14, med tilhørende forskrifter; forskrift om elektroniske kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) kapittel 9, samt forskrift om autorisasjon for installatør av elektronisk kommunikasjonsnett og radioutstyr (autorisasjonsforskriften) kapittel 9.

6.5.4 Nødnett

Utbyggingen av et felles nødnett for brann, politi, helse, samt andre etater med beredskapsoppgaver er kraftig forsinket i henhold til opprinnelig plan. Bruk av nødnett for å dekke kraftforsyningens behov for mobilt samband til beredskapsformål er heller ikke avklart i tilstrekkelig grad.

NVE har derfor konkludert med følgende:

- For å opprettholde nødvendig beredskap skal kraftforsyningen etter behov holde ved like, anskaffe og bygge radionett for mobilt samband (driftsradio) til beredskapsbruk uavhengig av nødnettets utbygging.
- Enhetenes behov for mobilt samband skal vurderes etter beredskapsforskriftens krav til nødvendig samband for ledelse og drift.
- Systemer som benyttes for mobilt samband skal tilfredsstille kravene i denne bestemmelsen.

Se Direktoratet for nødkommunikasjon (dNk) for ytterligere informasjon om utbygging av felles nødnett.

§6-6 Relésamband - vern av kraftsystem

Kommunikasjonsbaserte vernsystemer i sentral- og regionalnett skal ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet, og sørger for overføring av nødvendige signaler og meldinger mot relevante driftssentraler.

Vernsystemer skal sørge for rask og selektiv frakopling av enhet med funksjonsfeil for å begrense konsekvensen av feil i kraftforsyningssystemet.

Veiledning

Denne paragrafen omfatter sambandskrav til kommunikasjonsbaserte distansevern i sentral- og regionalnett. Krav til vern er ellers regulert av forskrift om systemansvaret i kraftsystemet (FOR-2002-05-07-448)§§ 20 Vern og reléplanlegging og 21 Systemvern.

Dette sambandet, her kalt relésambandet, inngår i vernesystemer basert på utveksling av informasjon mellom reléer som er plassert på ulike steder i kraftsystemet, slik at feilstedet blir funnet og feilbefengt anleggsdel hurtigst mulig blir frakoblet.

6.6.1 Systemkrav

Relésambandet må ha meget høy tilgjengelighet slik at det alltid fungerer i den brøkdelen av et sekund kraftsystemet er i feiltilstand. Feilstedet må kunne bestemmes og den feilbefengte anleggsdel utkobles. Dette bør skje i løpet av maksimalt 100 millisekunder for å unngå skader og fare for ukontrollerbare utkoblinger og ustabile tilstander i kraftsystemet.

Feil i kraftsystemet må ikke medføre samtidig svikt i vernet som skal initiere de nødvendige frakoblingene. Det må derfor være full uavhengighet mellom det utstyret som relésambandet benytter og de anleggsdelene relévernet skal beskytte.

6.6.2 Sikringstiltak

Vern er et av de viktigste bruksområdene for mange av de sambandene – jfr. driftskontrollsystemene, som betjener kraftsystemet, og stiller strenge krav til disse.

Generelt må relésambandet konstrueres for å fungere under alle de påkjenningene på kraftsystem og sambandssystem som kan forekomme, eksempelvis i forbindelse med uvær/lynnedslag eller strømutfall.

De viktigste tiltakene for å sikre at disse sambandssystemene til enhver tid er tilgjengelige for relévernet, er som for relevant samband og driftskontrollsystemer forøvrig.

Det vises her til tidligere paragrafer – særlig § 5-5 og § 6-4.

Kap 7 Øvrige bestemmelser

Bestemmelsene i dette kapitlet inneholder ulike bestemmelser som ikke naturlig hører hjemme i de foregående kapitlene, blant annet bestemmelser om rapportering, overtredelsesgebyr og dispensasjon.

§7-1 Rapportering

Alle enheter i KBO skal innrapportere ekstraordinære situasjoner til Norges vassdrags- og energidirektorat, herunder ulovlig fotografering, inntrengning, tyveri, hærverk og sabotasje eller forsøk på slik virksomhet, samt havarier, uhell og ulykker av betydning for drift og sikkerhet.

Veiledning

NVE har behov for statusrapporter for å kunne holde oversikt over situasjonen, bidra med informasjon og koordinering, rapportere til overliggende myndigheter, kontrollere at situasjonen følges opp på en tilfredsstillende måte og liknende.

Innenfor KBO finnes det tre typer rapporteringer/varslinger:

Varsling om at en ekstraordinær situasjon er oppstått og pågår

Statusrapportering under pågående ekstraordinær situasjon

Rapportering i etterkant av en ekstraordinær situasjon

Mal for rapportering finnes på www.nve.no.

7.1.1 Varsling til NVE om oppstått og pågående ekstraordinær situasjon

- Hensikten med varsling av pågående ekstraordinære situasjoner er å legge til rette for rask og effektiv håndtering av slike situasjoner i KBO-strukturen. NVE skal varsles dersom det oppstår hendelser som blant annet:
- Rammer eller kan ramme viktige deler av kraftinfrastrukturen.
- Rammer eller kan ramme to eller flere selskaper.
- Rammer driftskontrollsystemer i klasse 3.
- Ikke kan håndteres av den enkelte KBO-enhet.
- Gir eller potensielt kan gi store samfunnsmessige konsekvenser.
- Sikkerhetstruende handlinger.

7.1.2 Rapportering i etterkant

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

Enheten bør uten unødig opphold ved ekstraordinære situasjoner av lokal karakter rapportere til NVE.

Eksempler på fysiske hendelser og handlinger:	**Eksempler på større IKT-hendelser og handlinger:**
Store skader eller alvorlige forsøk på å skade anlegg Større strømbrudd eller risiko for dette Inntrengning og/eller tyverier Sabotasje	Datainnbrudd Systematiske forsøk på datainnbrudd Tjenestenektsangrep Funksjonssvikt i viktige IKT-systemer

Det er utarbeidet to skjemaer for rapportering. Disse finnes på www.nve.no, og er:

- Skjema for hendelser forårsaket av uvedkommende, se vedlegg.
- Skjema for hendelser forårsaket av teknisk svikt, uhell, ulykker, naturgitte forhold osv, se vedlegg.

Dersom skjemaene ikke benyttes, bør meldingen inneholde:

- Enhetens navn og adresse.
- Navn til enhetens leder, beredskapsleder og beredskapskoordinator.
- Nøyaktig steds- og tidsangivelse.
- Kortfattet beskrivelse av:
  - Hva som skjedde.
  - Type anlegg.
  - Forebyggende tiltak som er/var gjennomført.
  - Selskapets evne til å håndtere hendelsen.
  - Selskapets evne til å gjenopprette funksjon.
  - Gjenopprettingstiltak som er/ble gjennomført.
  - Motivet med hendelsen, dersom den er påført av uvedkommende.
  - Konsekvenser for samfunnet og selskapet.
  - Selskapets vurdering av hendelsen.
  - Annen relevant informasjon.
- Informasjon om hendelsen er meldt til politi/lensmann
- Informasjon om identitet til den/de som har forårsaket hendelsen, dersom det er aktuelt.
- Årsaksreduserende og/eller konsekvensreduserende tiltak som er iverksatt etter situasjonen.

Rapporten sendes per post til NVE Beredskapsseksjonen, eller per e-post til beredskapsrapportering@nve.no (passordbeskyttet/kryptert etter behov). Dersom det er viktig med rask kontakt, kan NVE nås på den døgnåpne beredskapstelefonen 22 95 93 60 / 909 92 231. I kontortid kan Beredskapsseksjonen kontaktes.

7.1.3 Rapporteringsrutiner

Enheten bør utarbeide en rapporteringsrutine som definerer hvilke ekstraordinære situasjoner enheten skal rapportere eller varsle NVE om.

Dersom enheten er i tvil om en hendelse skal rapporteres eller ikke, oppfordres enheten til å ta direkte kontakt med NVE for å avklare dette.

Rapportering til NVE gjøres i tillegg til, og ikke istedenfor, anmeldelse til politiet.

§7-2 Tilskudd til sikringstiltak og anskaffelse av reservemateriell

Norges vassdrags- og energidirektorat kan etter søknad gi tilskudd til sikringstiltak og anskaffelse av reservemateriell.

Veiledning

For tiden gir ikke NVE tilskudd til sikringstiltak og reservemateriell. Etter energiloven § 9-4 må virksomheter som omfattes av beredskapsforskriften, og som er pålagt å iverksette sikringstiltak, selv bekoste aktuelle beredskaps- og sikringstiltak.

Der NVE tidligere har gitt tilskudd til reservemateriell gjelder: Vilkår for tildeling og forvaltning av materiellet, se www.nve.no. Oversikt over materiellet finnes i databasen til e*Beredskap*, www.eberedskap.no.

§7-2 a Overtredelsesgebyr

§ 7-2 a. Ved overtredelse av bestemmelsene i § 1, § 2-4, § 3-1, § 3-2 og § 3-4 til § 3-8, § 4, § 5-1, § 5-2 og § 5-4 til § 5-7, § 6 og § 7-1 kan det ilegges overtredelsesgebyr.

Veiledning

Hensikten med overtredelsesgebyr er å sikre etterlevelse av regelverket. Overtredelsesgebyr etter beredskapsforskriften er en sanksjon som kan benyttes mot brudd på de av beredskapsforskriftens bestemmelser som er særskilt nevnt i bestemmelsen i § 7-2 a, i henhold til energiloven §§ 10-7 og 10-8. I tillegg er det adgang til å ilegge overtredelsesgebyr for brudd på energiloven kapittel 9.

Overtredelsesgebyr er en administrativ sanksjon som skiller seg fra straff ved at det er forvaltningen (NVE) og ikke domstolene/politiet som ilegger reaksjonen. Overtredelsesgebyr medfører at enheten blir pålagt å betale et pengebeløp som sanksjon for en overtredelse. Overtredelsesgebyr er altså tilbakeskuende, det vil si en reaksjon på noe som har skjedd.

Vedtak om overtredelsesgebyr er et enkeltvedtak. For å treffe vedtak om å ilegge overtredelsesgebyr kreves det:

- At den handlingen som er begått rent objektivt rammes av pliktregel som er nevnt i denne bestemmelsen.
- At det foreligger subjektiv skyld, det vil si enten forsett eller uaktsomhet

- At NVE finner at overtredelsesgebyr bør ilegges.

At handlingen rent objektivt rammes av en pliktregel, betyr at det rent faktisk kan konstateres at en plikt er overtrådt. For eksempel vil det klart rammes av rapporteringsplikten i § 7-1 dersom en enhet unnlater å rapportere om et havari av et klassifisert anlegg. Siden denne bestemmelsen er nevnt i § 7-2a, kan overtredelse bli sanksjonert med overtredelsesgebyr.

På energilovens område vil de fleste overtredelser begås av foretak. For at et foretak skal kunne ilegges gebyr, må det også foreligge skyld, i form av forsett eller uaktsomhet, hos enkeltperson(er) som handler på vegne av foretaket. For uoverlagte uhell og særlige omstendigheter som ikke er under menneskelig kontroll, som for eksempel naturkatastrofer, kan ikke foretak ilegges overtredelsesgebyr.

Vurderingen av om overtredelsesgebyr bør ilegges foretak skjer med utgangspunkt i de momenter som er nevnt i energiloven § 10-8 om overtredelsens grovhet mv.

Overtredelsesgebyrets størrelse fastsettes av NVE etter en skjønnsmessig og konkret vurdering. Blant annet skal det ved utmåling av overtredelsesgebyr tas hensyn til at overtredelsen:

- Ikke skal lønne seg.
- Skal være merkbar.
- Gebyrets størrelse vil kunne avhenge av selskapets økonomiske stilling.

§7-3 Klage på vedtak

Vedtak fattet av Norges vassdrags- og energidirektorat kan påklages til departementet. Klagen stiles til departementet, og sendes Norges vassdrags- og energidirektorat til forberedende klagebehandling.

Veiledning

Bestemmelsen opplyser om den generelle muligheten parter og andre med rettslig klageinteresse har på enkeltvedtak fattet under utøving av offentlig myndighet etter Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven LOV-1967-02-10) § 6.

Det er bare avgjørelser som er enkeltvedtak etter forvaltningsloven som kan påklages. Enkeltvedtak som er fattet med hjemmel i beredskapsforskriften kan, etter forvaltningsloven § 29, påklages til OED innen tre uker fra det tidspunktet underretningen om vedtaket er kommet frem til vedkommende part. Nærmere vilkår for klagerett er regulert i forvaltningsloven § 6.

En eventuell klage innebærer ikke uten videre at gjennomføringen av vedtaket utsettes. NVE kan beslutte å gi en klage utsettende virkning, etter forvaltningsloven § 42. Enheten kan ikke gå ut fra at utsettelse vil bli gitt i perioden klagen blir behandlet.

§7-4 Dispensasjon

Norges vassdrags- og energidirektorat kan i særlige tilfeller dispensere fra denne forskrift.

Veiledning

Det kan forekomme spesielle forhold der det kan være rimelig å gi dispensasjon fra reglene i denne forskriften. Bestemmelsen gir NVE myndighet til å beslutte at det kan gis dispensasjon gjennom bruk av enkeltvedtak.

Det er ikke mulig å gi generell veiledning for hvilke særlige tilfeller det vil bli gitt dispensasjon. Behovet for å fravike forskriftens krav må vurderes fra sak til sak. Det kan settes vilkår for en dispensasjon. Økonomiske betraktninger vil i svært liten grad gi grunnlag for dispensasjon. Bestemmelsen vil bli praktisert strengt.

Sentrale begreper

Beredskapsorganisasjon – Beskrivelse av hvordan enheten vil organisere sitt beredskapsarbeid i daglig drift og i beredskapssituasjoner.

Ekstraordinære situasjoner – en situasjon som går utover det enheten normalt er i stand til å håndtere innenfor daglige vakt- og beredskapsordninger.

Enhet – er i denne veiledningen kort for ”enhet i KBO”

Informasjonssikkerhet – Forebyggende tiltak som sikrer konfidensialitet, integritet og tilgjengelighet til sensitiv og gradert informasjon gjennom dens levetid.

Kraftforsyningsanlegg - anlegg for produksjon, transformering og distribusjon av elektrisk energi og fjernvarme, samt driftskontrollsystemet for å styre og overvåke anleggene.

N÷1-kriteriet - er et redundanskrav for drift i fjernvarmenett, sentralnettet og deler av regionalnettet. Det betyr at det er innebygd reserver i systemet slik at systemet skal tåle ethvert utfall av den største enheten (kjele, transformator, kabel, kraftledning etc.) uten å gi avbrudd.

Redundans - betyr å ha en ekstra enhet for å etablere en sikkerhetsmargin mot feil på systemet. Det betyr at dersom en feil eller en hendelse kan sette et system ut av spill, skal et annet system kunne overta viktige funksjoner. Ingen enkeltfeil eller hendelse skal kunne sette den viktige funksjonen ut av drift fordi man har en (normalt inaktiv) ressurs som står klar til å ta over hvis en primærressurs feiler.

Redundant - En komponent er redundant når den er i tillegg til det som er helt nødvendig. Et system er redundant når det har innebygd sikkerhet mot svikt, ved at redundante komponenter overtar funksjon ved svikt i hovedsystemet. Avhengig av akseptabel nedetid, kan den redundante komponenten være permanent tilkoblet eller være reserve for utskifting ved feil.

Eks.: Er varmesirkulasjonen i et fjernvarmesystem kritisk avhengig av en sirkulasjonspumpe, skal denne ha en reserve som kan overta.

Sensitiv informasjon – informasjon som kan brukes til å skade eller hindre kraftforsyningens funksjoner.

Uønskede handlinger - en tilsiktet eller utilsiktet handling/forsøk på handling som fører til en uønsket hendelse.

Uønskede hendelser - en hendelse som kan medføre tap av eller skade på kraftforsyningsanlegg, forsyningen av elektrisk kraft og fjernvarme, driftskontrollsystem, menneskelige og materielle beredskapsressurser og sikringstiltak, samt sensitiv, viktig og gradert informasjon.

Forkortelser

Forkortelse	Fullt navn
AMS	Avanserte måle- og styringssystemer
BFH	Bærefrekvens på høyspentlinjer
BfK	Beredskapsforskriften
BHK	Beredskapshåndbok for kraftforsyningen
c/c	Senter/senteravstand
CPNI	National Centre for the Protection of National Infrastructure (UK)
dB	Decibel
DMZ	Demilitarized Zone
dNk	Direktoratet for nødkommunikasjon
DSB	Direktoratet for samfunnssikkerhet og beredskap
EMC	Electromagnetic compability
EMI	Elektromagnetisk interferens
EMP	Elektromagnetisk puls
EN	Europeisk standard, European Norm
Energiloven	Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.
Energilovforskriften	Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.
Enfo	Energiforsyningens fellesorganisasjon
ENV	European Prenorm/Prestandard Foreløpig europeisk standard/Europanorm
EU	Europeiske Union
FEF	Forskrift om elektriske forsyningsanlegg
FG	Forsikringsselskapenes Godkjennelsesnemnd
FLO	Forsvarets logistikkorganisasjon
FOR	Forskrift
FoS	Forskrift om systemansvaret i kraftsystemet
GD	Gitterdør

Forkortelse	Fullt navn
GEO	Geosynchronous (or geostationary) orbits
GIS	Gassisolerte apparatanlegg, Gas Insulated Switchgear
GPS	Global Positioning System
H-EMP	High-altitude N-EMP
HF	Høyfrekvent
HMS	Helse, miljø og sikkerhet
HPM	High power microwave
HRV	Høyeste regulerte vannstand
ICS	Industrial Control Systems
IDS	Intruder detection system
IEC	International Electrotechnical Commission
IEMI	Intentional electromagnetic interference
IKT	Informasjons- og kommunikasjonsteknologi. I veiledningen omtalt som IT.
IPS	Intrusion protection system
ISBN	International Standard Book Number
ISF	Information Security Forum
ISO	International Organization for Standardization
IT	Informasjonsteknologi
KBO	Kraftforsyningens beredskapsorganisasjon
KD	Kraftverksdør
KP	Kraftverksport
KDS	Kraftforsyningens distriktssjefer
KFR	Kraftforsyningens fylkesrepresentant
KRS	Kraftforsyningens regionssjefer
KSL	Kraftforsyningens sentrale ledelse
L-EMP	Lyn - EMP
LRV	Laveste regulerte vannstand
LEO	Low Earth Orbits

Forkortelse	Fullt navn
NAV	Arbeids- og velferdsforvaltningen
NIS	Nettinformasjonssystem
NIST	National Institute of Standards and Technology
N2EMP	Non-nuclear EMP
NorSIS	Norsk senter for informasjonssikring
NS	Norsk standard
NSM	Nasjonal Sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OED	Olje- og energidepartementet
PEX	Kryssbundet polyetylenkabel
PIN	Personlig identifikasjonsnummer
PMR	Private Mobile Radio
PT	Post- og teletilsynet
RF-pakninger	Metallpakninger
RFW	Radio-Frequent Weapon
RL	Radiolinje
ROS	Risiko- og sårbarhet
ROV	Rometely operated vehicle
RSK	Retningslinjer for sikring av kraftforsyningsanlegg
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SGEMP	System generated Electromagnetic Pulse
SLA	Service Level Agreement eller Service Leveringsavtale
SS	Svensk standard
t = 10 millimeter	Tverrmål (tykkelse) = 10 millimeter
UPS	Uninterruptible Power Supply
US-CERT	United States Computer Emergency Readiness Team
UWB	Ultra Wide Band

Forkortelse	Fullt navn
VHF	Very High Frequency
VoIP	Voice over Internet Protocol, IP-telefoni
VPN	Virtual private network
VVS	Varme-, ventilasjons- og sanitærteknikk
Ø	Diameter

Forklaring til normer det er henvist til i § 5-5 med vedlegg.

ENV 1627 standard for innbrudds-/fasadesikring av dører, porter, vinduer, gitter, sjalusier mv. - er inndelt i 6 sikkerhetsklasser

For høyere krav (”strongrom” og fortifikasjon) gjelder standard EN 1143.

EN 356 standard for sikkerhetsglass - er inndelt i 5 klasser hærverkshemmende og over dette 3 klasser innbruddshemmende

For høyere krav (skuddsikkert) gjelder standard EN 1063.

EN 12320 standard for motstandsdyktighet hos hengelåser og hengelåsbeslag - er inndelt i 6 sikkerhetsklasser *)

EN 1303 standard for motstandsdyktighet hos faste låseenheter med tilbehør - er inndelt i 6 sikkerhetsklasser *)

For høyere krav (høysikkerhetslåser) standard etter EN 1300.

*) Låser og hengelåser er alternativt godkjent av ”Forsikringsselskapenes Godkjenningsnemnd” – **FG i 5** klasser

Forsvarsbygg som har utarbeidet en omfattende publikasjon (”Sikringshåndboka”) for beskyttelse av bygg og anlegg mot kriminalitet henviser til skallsikring (innbruddsikring) i 4 klasser hvor skallsikring 1 tilsvarer overnevnte sikkerhetsklasse 3 opptil skallsikring 4 som tilsvarer sikkerhetsklasse 6.

Denne veiledningen til BfK henviser kun til sikkerhetsklasser i dette intervallet – dvs. sikkerhetsklasse 3 – 6 i de EN som her er uthevet.

For enda bedre sikring opererer Forsvarsbygg med såkalt forsterket rom i ytterligere 4 klasser.

Der det er aktuelt angir denne veiledningen til BfK veiledende krav i klartekst ut fra bygningstekniske krav og beregningsmåter (f.eks. cm betong), det er her også vist til:

NS 3473 ”Prosjektering av betongkonstruksjoner” – beregnings- og konstruksjonsregler.

NS 3490 ”Prosjektering av konstruksjoner” - pålitelighet (jfr. konsekvenser av konstruksjoners sammenbrudd) - er inndelt i 4 pålitelighetsklasser

EN 13501 Brannmotstand er angitt som følger

Tall som 60, 90 og 120 - den tid i minutter vedkommende bygningsdel skal kunne opprettholde sine funksjoner ved nedennevnte påvirkninger (bokstavkoder):

E – integritet – motstå gjennombrenning

I – isolasjon – hindre spredning ved temperaturøkning på motsatt side av brannen

R – lastbærende funksjon – bygningsdelens (f.eks. vegg eller søyle) evne til å holde konstruksjonen oppe under brann

M – mekanisk styrke – bygningsdelens motstand mot slag fra fallende gjenstander o.l.

Sammenhengen mellom nye EN standarder og eldre standarder

ENV 1627 har erstattet NS 3170 slik at

ENV 1627 sikkerhetsklasse 3 tilsvarer NS 3170 sikkerhetsklasse 2

ENV 1627 sikkerhetsklasse 4 tilsvarer NS 3170 sikkerhetsklasse 3

osv.

EN 356 har erstattet NS 3217 mv - herunder.

EN 356 hærverkshemmende klasse P2A tilvarer NS 3214 (INSTA 151) A1

EN 356 hærverkshemmende klasse P3A tilvarer NS 3214 (INSTA 151) A2

osv

EN 356 innbruddshemmende klasse P6B tilvarer NS 3215 (INSTA 152) B1

EN 356 innbruddshemmende klasse P7B tilvarer NS 3215 (INSTA 152) B3

osv

FG ruter tilsvarer minst innbruddshemmende klasse B1

EN 1303 har erstattet NS 3620 slik at

EN 1303 sikkerhetsklasse 4 tilsvarer NS 3620 sikkerhetsklasse 3

EN 1303 sikkerhetsklasse 5 tilsvarer NS 3620 sikkerhetsklasse 4

osv.

EN 12320 har erstattet SSFN 014

EN 12320 sikkerhetsklasse 3 tilsvarer SSFN sikkerhetsklasse 2

EN 12320 sikkerhetsklasse 4 tilsvarer SSFN sikkerhetsklasse 3

osv.

NS 3473 ble i 2010 erstattet av EN 1992

NS 3490 ble i 2010 erstattet av EN 1990 ”

EN 13501 har erstattet NS 3919

Veiledning til forskrift om beredskap i kraftforsyningen

Vedlegg 1

Beredskapsrom

Norges vassdrags- og energidirektorat
2011

Innhold

1.1 § 6-4 Beredskapsrom

1.1.1.1 Utstyrsliste for beredskapsrom (6.4.6.1 Prosjektering)

Følgende utstyr bør være i/være i umiddelbar nærhet 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, minimum 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
- Punktlister formateres med stilen NVE punktliste
- Nummererte lister formateres med stilen NVE nummerert liste
- Lorum lipsum lei

Det skal foreligge oppdaterte utstyrslister, og planer for utstyr som skal bli tilført.

1.1.1.2 Drift og vedlikehold (6.4.6.2)

Ved de rutinemessige inspeksjonene skal følgende kontrolleres:

Bygningsteknisk:

- Dører, luker og porter
- Vannlekkasjer
- Skader på betong
- Rustangrep på stålkonstruksjoner
- Fuktighetsangrep på trekonstruksjoner

Ventilasjon

- Ventilasjonsanlegg med prøvekjøring av ventilasjonsaggregat. Det kontrolleres at viftene for fredsventilasjon er i orden og at det ikke er ulyder i lagre, motor, vifter, med mer
- Ventiler av alle slag kontrolleres. Om nødvendig foretas demontering og rengjøring og innsetting av alle bevegelige deler og anleggsflater med silikonholdig olje

Sanitærinstallasjoner:

- Tilbakeslagsventiler i drens- og kloakksystemet, samt øvrig sanitærutstyr skal kontrolleres og rengjøres minst en gang hvert år.

Elektroteknisk anlegg:

- Sikringsskap, varmeovner, og belysningsutstyr
- Reservelager av sikringer, lysstoffrør og liknende kompletteres ved behov
- Nødstrømanlegg med prøvekjøring av aggregat (minimum 30 minutter med last, se instruksjonsbok)
- Smøring og nødvendig etterfylling av olje og drivstoff
- Batterier

Oppvarming og fuktighet:

- Regulering av elektriske ovner og varmebatteri må skje på grunnlag av erfaring på vedkommende sted
- På grunn av høy relativ fuktighet i sommerhalvåret bør luftmengden som suges inn reduseres mest mulig

Sjekke at inventar og utstyr er hensiktsmessig lagret og ikke skades av fuktighet.

1.1.1.3 Kontroll (6.4.6.3)

I tillegg til forannevnte inspeksjoner skal alle beredskapsrom kontrolleres minimum en gang hvert år for følgende:

- Dører, luker og porter - hengsler, vridere, inspeksjonsplugger og pakninger
- Overtrykksmåler prøves ved å åpne og lukke reguleringsventilene når ventilasjonsanlegget er i gang. Ved mistanke om at måleren ikke viser rett, skal denne demonteres og sendes leverandøren for kontroll
- Sanitærutstyr med drens- og avløps-/kloakkledninger med sjokk og/eller tilbakeslagsventiler (om nødvendig foretas rengjøring)

- Brannslokkingsutstyr
- Sambandsopplegget, med prøving av utstyr

Når det ved beredskap beordres klargjøring av beredskapsrom, skal enheten gjennomføre fullstendig vedlikeholdsinspeksjon. Blant annet skal enheten funksjonsprøve og kontrollere at tekniske installasjoner virker slik det er forutsatt, og straks utbedre eventuelle mangler. Spesielt skal enheten:

- Teste sambandsutstyr
- Prøvekjøres ventilasjonsanlegg og nødstrømsaggregat
- Fylle vanntanker
- Vurdere behov for reserveproviant

Veiledning til forskrift om beredskap i kraftforsyningen

Vedlegg 2

Skjema, retningslinjer og enkeltvedtak

Norges vassdrags- og energidirektorat
2011

Innhold

VERNEPLIKTSVERKET

Melding/Søknad om fritak/utsettelse med fremmøte i Forsvaret ved mobilisering

1 Rapporterende ledds org kode:	2 Side nr.:	3 Meldingen/søknaden gjelder fra	mnd	år	Rapporterende ledd	UNNTATT FRA OFFENTLIGHET jf Off.loven § 5A og Forv.loven § 13 1. Ledd nr. 1 NÅR BLANKETTEN ER UTFYLT.

4 Linje nr	5 Op. kode	6 Fødsels-nummer	7 Grad befal	9 Krigstidsoppsetningskode Org kode i enhetsregisteret	10 Fritaks/uts gruppe	11 Utover 30 dager	12 Navn (etternavn, fornavn)	13 Sivil krigstids-oppsetning (kraftselskapet/everket)	14 Stilling/funksjon ved krigstidsoppsetning
01									
02									
03									
04									
05									
06									
07									
08									
09									
10									
11									
12									
13									
14									
15									
16									
17									
18									

Bl. 4071-B (Utg. 6-00 - kopi)

VERNEPLIKTSVERKET

Klage over avslag på søknad om utsettelse med fremmøte i Forsvaret ved mobilisering under gruppe 2 B

Til VERNEPLIKTSVERKET	Fra rapporterende ledd Norges vassdrags- og energidirektorat	Mobtermin

Fødselsnummer	Befalsgrad	Navn (Etternavn og fornavn)

Rulleførende enhet

Sivil krigstidsoppsetting

Sivil stilling/funksjon

Opplysninger om bemanningsforholdene ved krigstidsoppsettingen (besvares så nøyaktig som mulig)

1. Antall ansatte totalt:
2. Antall ansatte av samme kategori som påklagede:
3. Antall ansatte som er vernepliktige:
4. Antall ansatte av samme kategori som påklagede som er vernepliktige:
5. Antall ansatte som har fått fritak/utsettelse tidligere:
6. Antall ansatte av samme kategori som påklagede som har fritak/utsettelse:
7. Antall ansatte av samme kategori som påklagede som må disponeres av krigstidsoppsettingen ved mobilisering:
8. Krigstidsoppsettingens prioritet i offentlig beredskapsplan (fylles bare ut ved privat virksomhet)

Rapporterende ledds redegjørelse om hvorfor funksjonen til den person klagen gjelder ikke kan sløyfes eller dekkes ved omdisponering av ikke vernepliktig arbeidskraft ved mobilisering.

Sted og dato	Underskrift
	Stilling

Bl. 4072 B (Utg 5-91)

Vedlegg: Blankett 4071 B med utfylt tilgangsmelding for den påklagede

Informasjonssikkerhetspolicy
for
«Kraftselskapet»

Informasjonssikkerhet

«Kraftselskapet» forvalter kraftsensitiv informasjon på vegne av samfunnet. Slik informasjon omfattes av beredskapsforskriftens bestemmelser om beskyttelse. Informasjon som behandles for å ivareta driften er verdifull for «kraftselskapet» og må behandles og sikres deretter. Informasjonssikkerhet i «kraftselskapet» omfatter tiltak som bidrar til å oppfylle forskriftskrav, verne verdier og informasjon, samt evnen til å løse prioriterte oppgaver, gjennom å sikre:

- Konfidensialitet, som innebærer at ingen skal ha tilgang til informasjon uten tjenstlig behov.
- Integritet, som innebærer at informasjon og systemer skal være korrekt og pålitelig.
- Tilgjengelighet, som innebærer at informasjon og systemer skal være tilgjengelig for autoriserte brukere ved behov.

Mål for informasjonssikkerhet

Målet for informasjonssikkerhetsarbeidet i «kraftselskapet» er å sikre og å verne

- kraftsensitiv informasjon som fastsatt i beredskapsforskriften
- «kraftselskapet»s evne til å løse prioriterte oppgaver og tjenester
- integriteten og konfidensialiteten til «kraftselskapet»s informasjon

mot ulovlige handlinger og uønskede hendelser.

Her kan selskapet selv legge inn mer konkrete mål for informasjonssikkerhet. Noen eksempler på mer konkrete mål kan være:

- *Ingen ukontrollerte stopp eller sambandsbrudd knyttet til viktige IKT-system*
- *Andre mål knyttet til tilgjengelighet for systemer og informasjon*
- *Mål for brudd på konfidensialitet og integritet*

Viktige prinsipper

- God sikkerhet skal bygges på riktige holdninger blant medarbeiderne,
- Sikringstiltak skal iverksettes minst i henhold til beredskapsforskriftens krav til beskyttelse av kraftsensitiv informasjon.
- Risiko skal identifiseres gjennom risiko- og sårbarhetsanalyser (ROS-analyser).

- ROS-analysene skal oppdateres hvert år og ved større endringer
- Nye trusler skal vurderes og håndteres fortløpende.
- Sikkerhetstiltak skal til enhver tid ivareta beredskapsforskriftens krav, og for øvrig stå i forhold til det som er fastsatt som «kraftselskapet»s akseptable risikonivå.
- Dersom uønskede hendelser inntreffer, skal beredskapstiltak bidra til å begrense skaden og raskt komme tilbake til normal drift. Ekstraordinære situasjoner skal meldes NVE, jfr beredskapsforskriftens § 7-1.
- Sikkerhetsarbeidet skal integreres i arbeidet i linjen.
- Alle ansatte skal få nødvendig opplæring for å ivareta sitt sikkerhetsansvar.
- All tilgang til informasjon og verdier skal være basert på tjenstlig behov.

Ansvar og roller

Styret/ Daglig leder fastsetter policy for informasjonssikkerhet i «kraftselskapet». Styret fastsetter konkrete mål for «kraftselskapet»s sikkerhetsnivå og skal ha en årlig status for disse.

Informasjonssikkerhetsansvarlig er ansvarlig for å utarbeide og oppdatere «kraftselskapet»s policy og regelverk for informasjonssikkerhet og for holdningsskapende aktiviteter i «kraftselskapet». Denne skal bistå ved gjennomføring av sikringstiltak og ved oppfølging av sikkerhetsbrudd.

Den enkelte medarbeider i «kraftselskapet» er ansvarlig for å følge bestemmelsene i beredskapsforskriften og øvrige vedtatte sikkerhetsregler. Vedkommende skal varsle nærmeste leder ved sikkerhetsbrudd eller mistanke om brudd.

Eier av et informasjonssystem eller IKT-infrastruktur er ansvarlig for at systemet tilfredsstiller «kraftselskapet»s behov for funksjonalitet, sikkerhet og kvalitet og skal sørge for at oppgavene knyttet til systemet er ivaretatt. Eier av et system er den organisatoriske enheten som primært bruker systemet (største brukers prinsipp).Eier skal også sørge for at beredskapsforskriftens bestemmelser følges.

Linjeleder har ansvar for sikkerheten innen egen organisatoriske enhet.

Underskrift av daglig leder/ styreleder

TAUSHETSERKLÆRING VED ANSETTELSE/OPPDRAG I NORSK KRAFTFORSYNING

NAVN…………………………………………. ……………………………………….

PERSONNR. (11 SIFFER)…………………………………………………………………

FIRMA…………………………………………………………………………………...

ANSATT I/OPPDRAG FOR…SELSKAPET…………………………………………….

1. Jeg forstår at jeg i forbindelse med ansettelse i/oppdrag for kraftforsyningen kan få kjennskap til informasjon om

- forretningsanliggender, personopplysninger m.v.
- sensitiv informasjon om kraftforsyningen som kan brukes til å hindre eller skade kraftforsyningens funksjoner, jfr. forskrift om beredskap i kraftforsyningen (beredskapsforskriften) §§ 6-1 og 6-2.

2. Jeg har satt meg inn i

- beredskapsforskriften, særlig §§ 6-1 og 6-2.
- SELSKAPETs interne sikkerhetsbestemmelser og instrukser.

3. Jeg forplikter meg til

- å overholde bestemmelsene i beredskapsforskriften §§ 6-1 og 6-2 ved å beskytte sensitiv informasjon om kraftforsyningen
- å overholde de lokale sikkerhetsbestemmelsene
- å påse at informasjon som er underlagt personopplysningsloven ikke gis ut til andre enn de som i kraft av sin rolle har tilgang til disse
- å sørge for nødvendig konfidensialitet rundt opplysninger av betydning for virksomheten og konsernet for øvrig, herunder forretningsstrategi, utviklingsplaner og systemer
- ikke å bruke informasjon tilegnet i SELSKAPET i konkurrerende virksomhet
- å vise aktsomhet i min omtale av mindre viktig informasjon både i og utenfor SELSKAPET.
- å underrette SELSKAPET dersom jeg får et annet oppdrag, og det kan oppstå habilitetskonflikt.

4. Jeg er klar over

- at brudd på taushetsplikten kan medføre straffeansvar, bl.a. etter straffeloven §§ 294 og 405a, og lov om kontroll med markedsføring §§ 7 og 8.
- at taushetsplikten også gjelder etter at ansettelse/oppdrag er avsluttet, jfr. forvaltningsloven § 13 f.

Sted og dato ……………………………………………………

Underskrift…………………………………………………………..

Norges
vassdrags- og
energidirektorat
NVE

Taushetsplikt etter BfK § 6-2
Unntatt offentlighet etter offl. § 13 1. ledd
(ferdig utfylt)

Melding om klassifisering av anlegg

Fyll inn i de grå feltene og skriv ut skjemaet for underskrift

Side 1 av 2

1. Type anlegg:

Driftkontrollsystem Transformatorstasjon Kraftstasjon Fjernvarmeanlegg Ledning/kabel

2. Systemets/anleggets navn:

i kommune i fylke

3. Systemets/anleggets eier:	**Organisasjonsnummer:**
4. Anlegget drives av (dersom annen enn eier)**:**	**Organisasjonsnummer:**

5. Kryss av for hvilke endringer som meldes inn
(energiloven § 6-2, beredskapsforskriften § 6-3, jf energiloven § 6-6).

Nybygg Ombygging Endring Utvidelse av (spesifiser):

Opplysninger om anlegget	**Bilag nr**
6. Tegninger/opplysninger som viser hva anlegget/systemet skal styre/overvåke/forsyne (prinsipielt kontrollbilde)	
7. Anlegget/systemet inngår i hvilke nettnivåer / tilknytning til nettet: (kryss av det som passer) Sentralnett Regionalnett Distribusjonsnett Fjernvarmenett	
8. Anlegget/systemets viktighet for omkringliggende nett (evt. redundans i systemet)	
9. Antall avganger på underliggende nett:	
10- Anlegget/systemet forsyner/betjener: Antall forbrukere Antall transformatorstasjoner Antall kraftstasjoner Antall fjernvarmeanlegg Annet (spesifiser):	
11. Transformatorstasjon Samlet ytelse (MVA) av installasjonen: a. Nåværende installasjon: stk á MVA / kV/kV stk á MVA / kV/kV Total ytelse: MVA b. Endelig installasjon stk á MVA / kV/kV stk á MVA / kV/kV Total ytelse: MVA	

12. Kraftstasjon Samlet ytelse (MW) av installasjonen: a. Nåværende installasjon: stk á MW kV stk á MW kV Total ytelse: MW b. Endelig installasjon stk á MW kV stk á MW kV Total ytelse: MW **13. Fjernvarmeanlegg** Samlet installert effekt: MW **14. Ledning/kabel** Spenning: Lengde: Type:	
15. Omfang av forsyning/viktige forsyningsobjekter. Angivelse av viktige forsyningsobjekter (industri, totalforsvarsanlegg, offentlig adm., helseinstitusjoner m.v.)	
Har planene for anlegget vært drøftet med NVE? Hvis ja – hvilken seksjon?	
Tidsplaner Anlegget antas påbegynt dato: Anlegget antas satt i drift dato:	
Andre opplysninger:	
Kontaktperson om anlegget: Navn: Tittel: Telefon: E-postadresse: Postadresse:	
Det skal inngås en sikkerhetsavtale med de firmaer som står for levering og installasjon av styrings- og kontrollsystemer, samt data- og sambandsutstyr i anlegget/systemet.	

……………………………… ………………………… ………………………………..
Sted Dato Firmastempel

……………………………………………………………………………. …………………………………
Adresse Underskrift

RETNINGSLINJER FOR TUNGTRANSPORTBEREDSKAP I KRAFTFORSYNINGEN

Olje- og energidepartementet har 28. november 1995 fastsatt følgende retningslinjer for tungtransport i kraftforsyningen:

1. Behov for tungtransportberedskap

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

2. Statnett SFs rolle

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

3. Dekning av utgifter

Statnett SF skal administrere og organisere transportberedskapen og vedlikeholde den maskinpark transportberedskapen omfatter.

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

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

4. Klargjøringstid

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

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

5. Styring

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

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

Norges
vassdrags- og
energidirektorat
NVE

SIKKERHETSAVTALE FOR SENSITIV INFORMASJON

Sikkerhetsavtale er inngått mellom Norges vassdrags- og energidirektorat (NVE) og *SELSKAPET, Adresse….* i forbindelse med oppdrag eller liknende for NVE eller kraftforsyningen.

I medhold av Energiloven (LOV 1990-06-29 nr 50) kapittel 9. Beredskap og ”Forskrift om beredskap i kraftforsyningen” (FOR 2002-12-16 nr 1606), jf. offentleglova (LOV 2006-05-19 nr 16), har over nevnte parter inngått følgende sikkerhetsavtale:

I

SELSKAPET erklærer seg villig til å oppfylle de sikkerhetskrav som NVE har stilt i forbindelse med oppdraget som er angitt ovenfor. Disse skal være innen rammen av de lover og forskrifter som er nevnt ovenfor eller de rettelser og tilføyelser som måtte være gitt til disse av NVE, annen relevant myndighet, eller i samsvar med gjensidig avtale partene i mellom for å tilpasse sikkerhetsbestemmelsene til *SELSKAPET* sin virksomhet.

II

Informasjon det gis tilgang til skal være unntatt etter offentleglova § 13 første ledd såfremt det er informasjon som er underlagt taushetsplikt etter beredskapsforskriften § 6-2 om sensitiv informasjon om kraftforsyningen. Annen informasjon det gis tilgang til kan være omfattet av offentleglova § 21 om unntak av omsyn til nasjonale forsvars- og tryggingsinteresser eller § 24 om unntak for kontroll- og reguleringstiltak, dokument om lovbrot og opplysningar som kan lette gjennomføringa av lovbrot m.m.

III

Taushetserklæring innhentes fra personell hos *SELSKAPET* som kan få tilgang til sensitiv informasjon, jf beredskapsforskriften § 4-3 *Anskaffelser i kraftforsyningen*.

IV

SELSKAPET erklærer at de ikke vil utlevere eller bekjentgjøre sensitiv informasjon til andre i *SELSKAPET*, tredjepart, herunder underleverandører, konsulenter, målgrupper for markedsføring og media uten at NVEs samtykke på forhånd foreligger.

V

SELSKAPET forplikter seg til ikke å omtale eller gjøre kjent for noen negative avgjørelser i saker vedrørende andre leverandører, underleverandører, konsulenter, mv. uten NVEs samtykke i hvert enkelt tilfelle.

VI

SELSKAPET forplikter seg til å forvalte sensitiv informasjon på en slik måte at kravene til informasjonshåndtering stilt i beredskapsforskriften kap. 6 Informasjonssikkerhet blir ivaretatt. Dokumenter og lagringsmedium som tilhører NVE eller kraftselskapet skal tilbakeleveres etter at oppdraget er avsluttet.

VII

Denne avtalen forplikter ikke NVE økonomisk for dekning av utgifter eller krav *SELSKAPET* måtte ha for å oppfylle betingelsene i henhold til denne avtale. Det erkjennes imidlertid at partene i annen skriftlig form (kontrakt eller liknende) kan treffe avtale om dekning av slike omkostninger som følger av de sikkerhetskrav som er stilt eller som vil bli stilt til *SELSKAPET* under utførelsen av oppdraget.

VIII

SELSKAPET forplikter seg til straks å orientere NVE ved endring av firmanavn og daglig leder. Flytting av lokaliteter skal meddeles NVE *før* flyttingen finner sted.

IX

Partene forplikter seg til at sensitiv informasjon ved utløp av eventuell anbudsfrist og ved oppdragets slutt, blir tilbakelevert til oppdragsgiver.

X

Ved en eventuell gjeldsforhandling og konkurs forplikter *SELSKAPET* seg å orientere NVE. Dersom NVE finner de nevnte forhold sikkerhetsmessig betenkelige, vil prosjektet kunne termineres.

XI

Representanter for NVE har rett til å føre tilsyn med sikkerhetsforholdene i *SELSKAPET* sin virksomhet i tilknytning til eventuell sensitiv informasjon knyttet til oppdraget. Dersom vedkommende representant fastslår sikkerhetsmessige svakheter eller sikkerhetsmessige mangler innenfor virksomheten, skal *SELSKAPET* gis en skriftlig melding om forholdet eller forholdene med anbefalinger for å bedre sikkerhetstilstanden.

XII

Brudd på denne avtalen vil kunne medføre at oppdraget termineres, eventuell annen forføyning i ht. norsk lovgivning.

XIII

Forandringer i denne avtalen kan bare skje skriftlig og skal godkjennes av begge parter. Avtalen skal gjelde så lenge *SELSKAPET* deltar i oppdraget. Avtalen kan sies opp gjensidig med 30 - tretti – dagers skriftlig varsel, hvormed *SELSKAPET* innen varslets utløp er forpliktet til å avlevere til NVE sensitiv informasjon som *SELSKAPET* har mottatt eller utarbeidet.

XIV

Partenes rettigheter og plikter etter denne avtalen bestemmes i sin helhet av norsk rett.

XV

Denne avtalen er utferdiget i *to* eksemplarer. Hver av partene beholder *ett* eksemplar. Kopi av avtalen formidles eventuelle oppdragsgivere i kraftforsyningen.

Sted………….. Dato…………..	Sted………….. Dato……………..
……………………………………. Navn (blokkbokstaver)	………………………………………. Navn (blokkbokstaver)
……………………………………. (signatur)	………………………………………. (signatur)
For *SELSKAPET* Daglig leder	For Norges vassdrags- og energidirektorat (NVE) etter fullmakt
Stempel	Stempel

Org. nr… xxx yyy zzz

Hendelser forårsaket av teknisk svikt, uhell, ulykker, naturgitte forhold osv.

Enhetens/selskapets navn:		
Adresse:	Postnr.:	Poststed:
Telefon:	Telefaks:	E-post:
Leder:	Beredskapsleder:	
Beredskapskoordinator:		

Tids- og stedsangivelse for hendelsen:	Dato:	Kl.	Rapport nr:
Fylke:	Stedsnavn:		
☐ By	☐ Tettsted	☐ Landsbygd	Annet:

Type hendelse:	☐ Ulykke / uhell, hva:			
☐ Teknisk svikt		☐ Naturgitte forhold		
☐ Slitasje	☐ Mekanisk svikt	☐ Tordenvær	☐ Vann/nedbør	☐ Vegetasjon
☐ Varmgang	☐ Elektrisk feil	☐ Vind	☐ Flom	☐ Ras
☐ Materielltretthet	☐ Korrosjon	☐ Snø/is	☐ Forurensing	☐ Brann
☐ Annet:		☐ Fugl/dyr	☐ Annet:	

Medvirkende årsak(er):		
☐ Mennesker	☐ Driftspåkjenning	☐ Konstruksjon/montasje
☐ Eget personale	☐ Overbelastning	☐ Konstruksjonsfeil
☐ Innleid	☐ Høy/lav spenning	☐ Produksjonsfeil
☐ Andre	☐ Høy/lav frekvens	☐ Montasjefeil
☐ Feilbetjening	☐ Produksjonsutfall	☐ Feil innstilling/justering
☐ Trefelling	Annet:	Annet:
☐ Anleggsarbeid	☐ Drift / vedlikehold:	
☐ Trafikkskade	☐ Mangelfullt vedlikehold	☐ Mangelfulle avtaler
Annet:	☐ Manglende instrukser/rutiner	Annet:

Konsekvenser av hendelsen:		
Produksjon:	☐ Overføring/fordeling	☐
☐ Stopp	☐ Brudd	☐
☐ Innskrenkning	☐ Innskrenkning	☐
☐	☐	☐
Annet:		

Økonomiske konsekvenser av hendelsen:	
☐ Produksjonstap, ca kr.:	☐ Materielle kostnader, ca. kr.:
☐ KILE-kostnader, ca kr.:	☐ Arbeidskostnader, ca. kr.:
Annet:	

Hendelser forårsaket av teknisk svikt, uhell, ulykker, naturgitte forhold osv.

Objekt(er) som ble rammet av hendelsen:

Produksjonsanlegg:	**Nett:**		**Stasjoner tilknyttet:**
☐ **Vannkraft**	☐ **Sentralnett**	☐ **Gass**	☐ **Sentralnett**
☐ **Kraftstasjon**	☐ **Regionalnett**	☐ **Fjernvarme**	☐ **Regionalnett**
☐ **Rørgate**	☐ **Distribusjonsnett**	**Annet:**	☐ **Distribusjonsnett**
☐ **Dam**	☐ **300 – 400 kV**		☐ **300 – 400 kV**
☐ **Vindkraft**	☐ **132 – 220 kV**		☐ **132 – 220 kV**
☐ **Biobrensel**	☐ **32 – 66 kV**		☐ **32 – 66 kV**
☐ **Gass**	☐ **>1 – 22 kV**		☐ **>1 – 22 kV**
Fjernvarme / annet	☐ **Lavspenning**		☐ **Trafostasjon**
	☐ **Luftnett**		☐ **Koblingsstasjon**
	☐ **Kabelnett**		**Annet:**

Adm. bygning:	**Øvrige bygg:**		**Driftssentral:**	
☐ **Kontor**	☐ **Verksted**	☐ **Garasje**	☐ **Sentralnett**	☐ **Distribusjonsnett**
☐ **Datarom**	☐ **Lager**	☐ **Innhegning**	☐ **Regionalnett**	☐ **Kraftstasjon**
Annet:	**Annet:**		**Annet**	

Feilbeskrivelse:

☐ **Mekanisk feil**	☐ **Materiellteknisk feil**	☐ **Elektrisk feil**	**Annet:**

Utløsende årsak:

☐	☐	☐
☐	☐	☐

Analyse / vurdering:

Kortfattet beskrivelse av det inntrufne:

Kortfattet beskrivelse av forebyggende tiltak som er/var gjennomført:

Kortfattet beskrivelse av selskapets evne til å håndtere det inntrufne (administrativt, intern og ekstern info. osv.):

Kortfattet beskrivelse av gjenopprettingstiltak og selskapets evne til å gjenopprette funksjonalitet/utbedre skader (tilgang til personell, kompetanse, materiell, utstyr, osv.):

Kortfattet beskrivelse av samfunns- og selskapsmessige konsekvenser på grunn av det inntrufne:

Sted:	**Dato:**	**Signatur:**	**Antall vedlegg:**

Taushetsplikt etter BfK § 6-2
Unntatt offentlighet etter offl. § 13 første ledd

Hendelser forårsaket av uvedkommende

Enhetens/selskapets navn:		
Adresse:	Postnr.:	Poststed:

Telefon:	Telefaks:	E-post:

Daglig leder:	Beredskapsleder:
Beredskapskoordinator:	

		Kl.	Rapport nr:
Fylke:	Stedsnavn:		

☐ By	☐ Tettsted	☐ Landsbygd	Annet:

Type hendelse(er):

Vinningsforbrytelse	☐ Ja	☐ Nei	☐ Vet ikke	Bevisst handling	☐ Ja	☐ Nei	☐ Vet ikke

Inntrengning:	Skadeverk:	Hacking	Manipulering:
☐ Innbruddsforsøk	☐ Hærverk	☐ Vellykket inntregning	☐ Bestikkelser
☐ Innbrudd	☐ Brann	☐ Mislykket inntregning	☐ Trusler
☐ Mistenkelig nærvær	☐ Sabotasje	☐ Adm. system	☐ Avlyttning
☐ Fotografering	☐ Terror	☐ Driftskontr.system	☐ Uvanlig utspørring
Annet:	Annet:	Annet:	Annet:

Tap og evt. konsekvenser av hendelsen:

Tap av informasjon:	Materielle tap:		Konsekvenser:
☐ Driftssensitiv	☐ PC	☐ Materiell	☐ Fysisk skade
☐ Adm./øk.sensitiv	☐ Programvare	Hva:	Ca. kostnad:
☐ Personalsensitiv	Hva:	☐ Utstyr	☐ Ukjent omfang
Annet:	☐ Kommunikasjonsutstyr	Hva:	☐ Strømutfall
	Hva:	Annet:	Annet:

Objekt(er) som ble rammet av hendelsen:

Produksjonsanlegg:	Nett:		Stasjoner tilknyttet:
☐ Vannkraft	☐ Sentralnett	☐ Gass	☐ Sentralnett
☐ Kraftstasjon	☐ Regionalnett	☐ Fjernvarme	☐ Regionalnett
☐ Rørgate	☐ Distribusjonsnett	Annet:	☐ Distribusjonsnett
☐ Dam	☐ 300 – 400 kV		☐ 300 – 400 kV
☐ Vindkraft	☐ 132 – 220 kV		☐ 132 – 220 kV
☐ Biobrensel	☐ 32 – 66 kV		☐ 32 – 66 kV
☐ Gass	☐ >1 – 22 kV		☐ >1 – 22 kV
Fjernvarme / annet	☐ Lavspenning		☐ Trafostasjon
	☐ Luftnett		☐ Koblingsstasjon
	☐ Kabelnett		Annet:

Adm. bygning:	Øvrige bygg:		Driftsentral:	
☐ Kontor	☐ Verksted	☐ Garasje	☐ Sentralnett	☐ Distribusjonsnett
☐ Datarom	☐ Lager	☐ Innhegning	☐ Regionalnett	☐ Kraftstasjon
Annet:	Annet:		Annet	

Taushetsplikt etter BfK § 6-2
Unntatt offentlighet etter offl. § 13 første ledd

Hendelser forårsaket av uvedkommende

(Side 2 av 2)

pe, antall personer, antatt alder, andre kjennetegn, mm.):

Analyse / vurdering:

Kortfattet beskrivelse av det inntrufne:

Kortfattet beskrivelse av forebyggende tiltak som er/var gjennomført (fysisk sikring, overvåking, mm.):

Kortfattet beskrivelse av selskapets evne til å håndtere det inntrufne (administrativt, intern og ekstern info mm):

Kortfattet beskrivelse av gjenopprettingstiltak og selskapets evne til å gjenopprette funksjonalitet / utbedre skader (tilgang til mannskap, kompetanse, materiell, utstyr, osv):

Kortfattet beskrivelse av eventuelle samfunns- og selskapsmessige konsekvenser pga. det inntrufne:

Sted:	Dato:	Signatur:	Antall vedlegg:

Denne serien utgis av Norges vassdrags- og energidirektorat (NVE)

Utgitt i Veilederserien i 2011

Nr. 1	Veiledning til forskrift om beredskap i kraftforsyningen (136 s.)
Nr. 2	Utforming av konsesjonssøknad for fjernvarmeanlegg (22 s.)

Norges
vassdrags- og
energidirektorat

NVE

Norges vassdrags- og energidirektorat

Middelthunsgate 29
Postboks 5091 Majorstuen,
0301 Oslo

Telefon: 22 95 95 95
Internett: www.nve.no