Innhold

6. Informasjonssikkerhet 1
6.1 Identifisering av kraftsensitiv informasjon og rettmessige brukere 2
6.2 Kraftsensitiv informasjon 4
6.3 Beskyttelse, avskjerming og tilgangskontroll 16
6.4 Sikkerhetsinstruks 20
6.5 Anskaffelser 22
6.6 Begrenset anbudsinnbydelse 24
6.7. Personkontroll 27
6.8 Sikkerhetskopier 30
6.9 Digitale informasjonssystemer 32
6.10 Beskyttelse av brytefunksjonalitet i AMS 41

6. Informasjonssikkerhet

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

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

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

6.1 Identifisering av kraftsensitiv informasjon og rettmessige brukere

§

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

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

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

Med rettmessig bruker menes fysiske eller juridiske personer som har tjenstlig behov for kraftsensitiv informasjon. Den enkelte KBO-enhet skal selv avgjøre hvem som har tjenstlig behov for kraftsensitiv informasjon innenfor sin virksomhet.

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

Virksomheten plikter å identifisere hva som er kraftsensitiv informasjon:

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

Virksomheten plikter å identifisere hvor kraftsensitiv informasjon befinner seg:

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

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

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

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

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

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

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

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

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

Eksempel: Identifisering av kraftsensitiv informasjon

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

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

Eksempel: Rettmessig bruker og sikring av kraftsensitiv informasjon

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

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

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

Eksempel: Videreformidling av kraftsensitiv informasjon

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

6.2 Kraftsensitiv informasjon

§

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

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

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

a. Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband

b. Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg

c.	*Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift*
d.	*Oversikt over fordelingsnett til samfunnsviktige funksjoner. Oversikt over rørnett for fjernvarme til samfunnsviktige funksjoner*
e.	*Nøyaktig kartfesting av jordkabler. Nøyaktig kartfesting av rørnett i fjernvarmeanlegg med varmesentraler i klasse 2*
f.	*Forebyggende sikkerhetstiltak mot bevisst skadeverk*
g.	*Lokalisering av reserve driftssentraler og andre særskilte beredskapsanlegg for ledelse og drift*
h.	*Detaljerte analyser av sårbarhet som kan brukes til bevisst skadeverk.*
i.	*Beredskapsplaner for å håndtere bevisst skadeverk*
j.	*Samlet oversikt over reservemateriell, reserveløsninger eller reparasjonsberedskap av betydning for håndtering av bevisst skadeverk*

Bestemmelsen krever skjønnsmessig vurdering av informasjonseier eller behandler. Bestemmelsen

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

Taushetsplikt for kraftsensitiv informasjon

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

***Energiloven* § 9-3 *(Informasjonssikkerhet)* annet ledd**

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

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

Hva omfattes av den generelle definisjonen?

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

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

- Informasjonen må være «*spesifikk* og *inngående*». Med spesifikk menes konkret, for eksempel et konkret anlegg eller system. Med inngående menes detaljert. Dette stiller krav til at opplysningene må være mer enn kun oversiktspreget og ha en viss detaljeringsgrad. Bokstav a-j kommer nærmere inn på eksempler på hva som menes med spesifikke og inngående opplysninger i forskjellige tilfeller. Spesifikk og inngående opplysninger vil for eksempel kunne være en teknisk tegning eller bilde med detaljer av et klassifisert anlegg sammen med geografisk lokalisering eller navn på anlegget

- Informasjonen må videre være av en slik art at den *«kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen.»* Dette innebærer at misbruk av opplysningene til sabotasjeformål har et skadepotensial. Virksomheten trenger ikke å vite med sikkerhet at skade vil oppstå eller at funksjoner faktisk blir påvirket dersom dette skjer, men det er tilstrekkelig at virksomheten anser det som sannsynlig at misbruk av opplysningene *kan* få slike følger. Når konstruktive detaljer og tilgjengeligheten til anlegget er synliggjort, er det både spesifikk og inngående informasjon. Også sammenstilling av opplysninger, som alene ikke anses som sensitive, kan gi så spesifikk eller inngående informasjon om kraftforsyningen eller anlegg at den kan brukes til å skade anlegg, system eller annet, eller påvirke funksjoner på en måte som har betydning for kraftforsyningen

Eksempel: Informasjon som ikke er kraftsensitiv

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

Hva omfattes av listen i bokstav a – j?

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

<u>*Bokstav a*</u>

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

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

Eksempel: Kraftsensitiv informasjon og besøk på driftssentral

Nett AS har fått en forespørsel fra sin leverandør av driftskontrollsystem om han kan ta med noen utenlandske kunder hos denne leverandøren på besøk. Nett AS har nylig bygget ny driftssentral med et moderne driftskontrollsystem, klasse 3. Marie'L Ampere (beredskapsleder) vurderer at «systemer som ivaretar viktige driftskontrollfunksjoner», altså driftskontrollsystem er vidtrekkende. Det dekker eksempelvis koplingsbilder, skiftordning for personell, selve SCADA-systemet med skjermer og full oversikt over nett og produksjon, annet IT-utstyr på sentralen, fysisk låsesystem og soneinndeling, samt beredskapsrommet.

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

<u>*Bokstav b*</u>

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

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

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

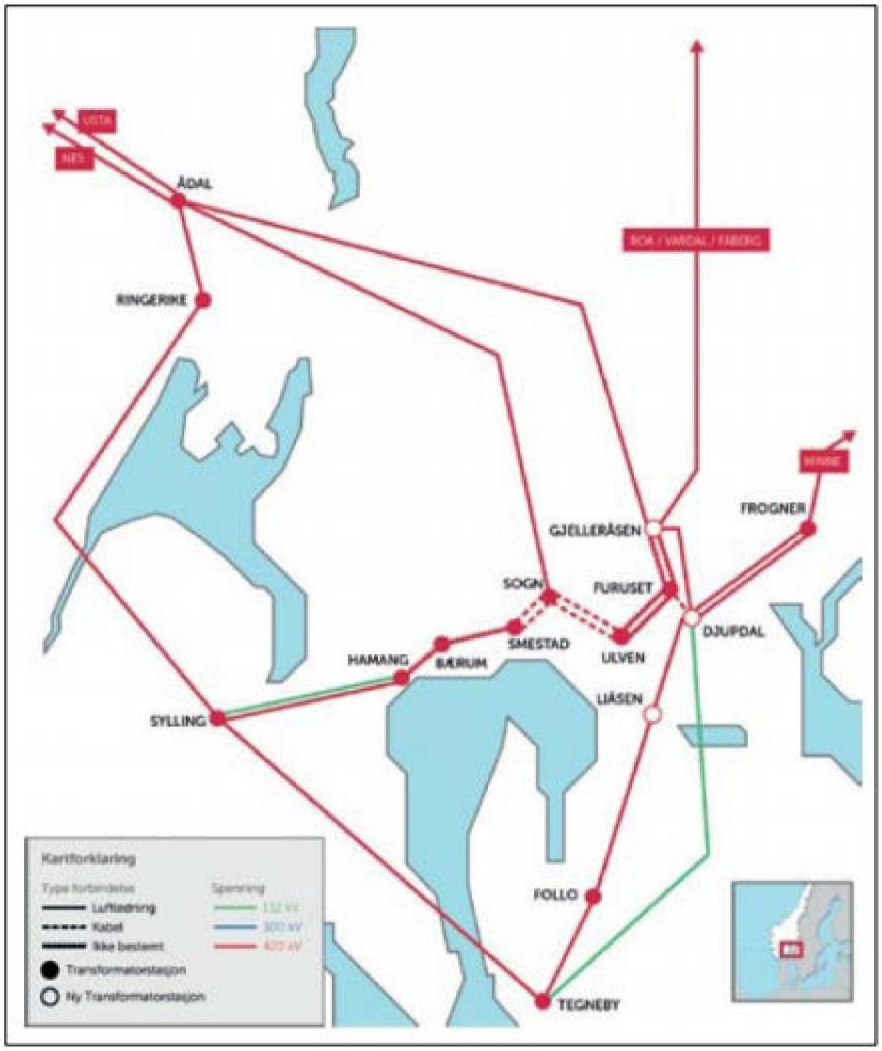
Enkle og lite detaljerte oversikter over kraftnettet på et aggregert nivå, vil falle utenfor hva forskriften definerer som kraftsensitiv informasjon Det at oversikten er aggregert betyr at den *ikke* viser brytere og samleskinner eller annen informasjon som gjør det mulig å utlede sensitive opplysninger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

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

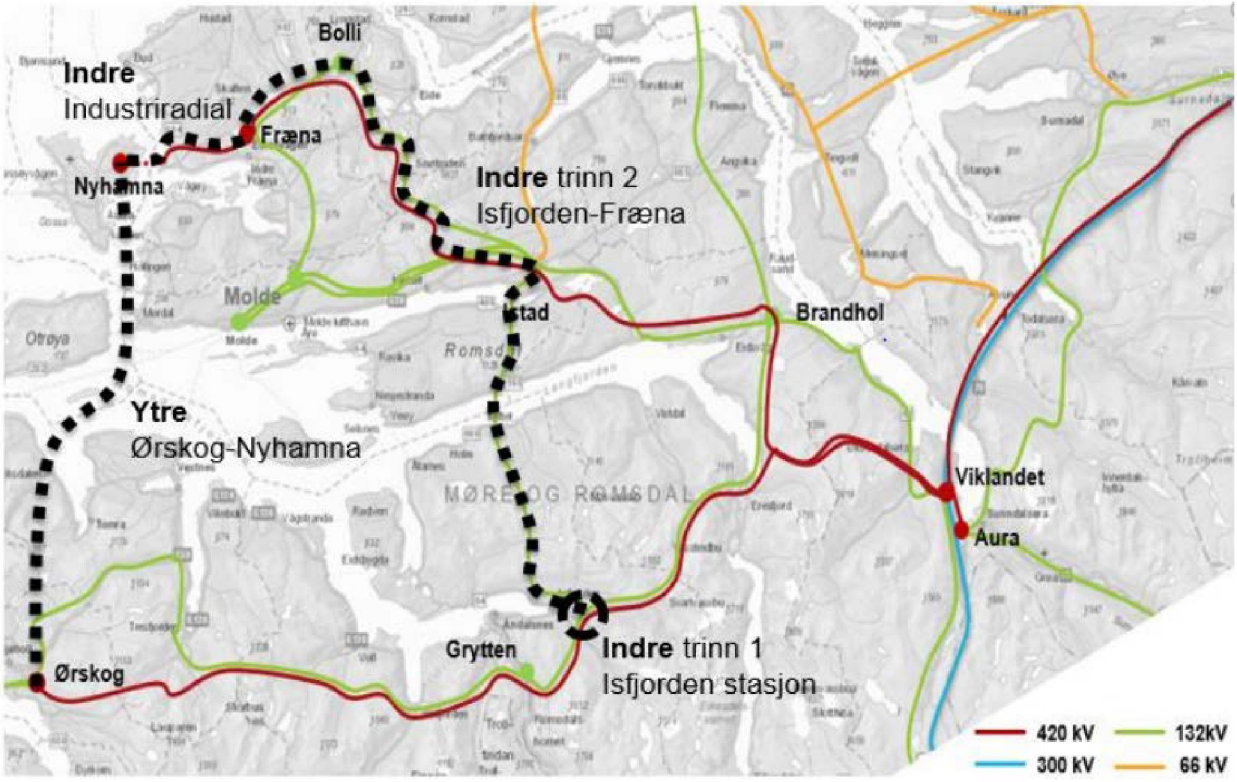
Eksempel: Oversiktskart som ikke er kraftsensitivt

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

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



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



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

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

Bokstav c

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

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

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

Eksempel: Generelle konsesjonssaker

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

Eksempel: BIM-modell

Vannkraft AS bygger ny transformatorstasjon. Entreprenøren har designet ny stasjon i BIM – Bygnings Informasjons Modellering. En slik BIM-modell av en transformatorstasjon kan inneholde kraftsensitiv informasjon da den er en digital speiling av en reell stasjon. BIM-modellen kan dermed ikke publiseres.

Bokstav d

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

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

Eksempel: Fordelingsnett til sykehus

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

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

Bokstav e

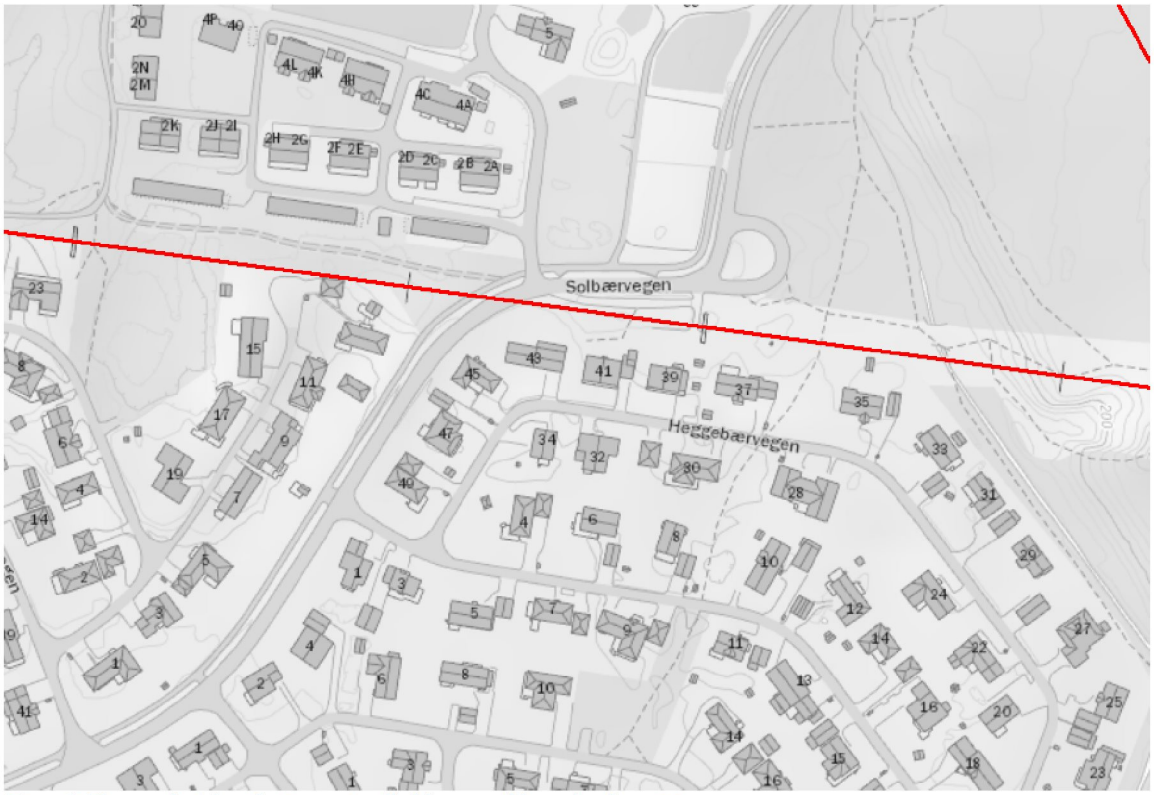
«Nøyaktig kartfesting av jordkabler. Nøyaktig kartfesting av rørnett i fjernvarmeanlegg med varmesentraler i klasse 2»

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

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

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

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



Figur 3 Eksempel på kartfesting av jordkabler som ikke er kraftsensitiv

Eksempel: Kartfesting av rørnett

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

Bokstav f

«Forebyggende sikkerhetstiltak mot bevisst skadeverk»

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

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

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

Bokstav g

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

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

Med særskilte beredskapsanlegg menes eksempelvis:

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

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

Eksempel: Reservedriftssentral

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

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

Bokstav h

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

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

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

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

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

Eksempel: Presentasjon på åpent brukermøte i regi av interesseorganisasjon

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

<u>*Bokstav i*</u>

«Beredskapsplaner for å håndtere bevisst skadeverk»

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

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

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

Eksempel: Beredskapsplan

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

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

Bokstav j

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

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

Eksempel: Database over samlet lagerbeholdning

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

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

Maler

Informasjonsikkerhetsavtale NVE-avtale mal på norsk og engelsk se NVE maler

NVEs mal for taushetserklæring på norsk og engelsk se NVE maler

Veiledere

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (norsk)

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (engelsk)

Metode for å finne kraftsensitiv informasjon på internett

Nettvett Sikker sletting

Krysskopling til annet regelverk

Lov om nasjonal sikkerhet (sikkerhetsloven)

6.3 Beskyttelse, avskjerming og tilgangskontroll

§

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

Virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle system og rutiner for effektiv avskjerming, beskyttelse og tilgangskontroll for kraftsensitiv informasjon. Beskyttelse skal omfatte tiltak mot avlytting og manipulering fra uvedkommende.

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

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

Ordforklaring

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

Hvordan oppfylle kravet

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

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

Tiltak som vurderes for tilgangskontroll og beskyttelse bør omfatte:

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

Se mer om tiltak under § 6-5.

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

Merking av kraftsensitiv informasjon

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

Merking av kraftsensitiv informasjon (Bokmål)	Merking av kraftsensitiv informasjon (Nynorsk)
Underlagt taushetsplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt fra innsyn etter offentleglova § 13.	Underlagd teieplikt etter energiloven § 9-3 jf. kbf. § 6-2. Unntatt frå innsyn etter offentleglova § 13.

Eksempel: Nyansatt

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

Tiltak og prosedyrer inngår i virksomhetens internkontrollsystem for informasjonssikkerhet.

Eksempel: Sikker sletting

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

Sikkerhetsregler for mobile enheter

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

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

Eksempel: Særskilte regler for beskyttelse av mobile enheter

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

Standarder

- NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav

Veiledere

- Digitaliseringsdirektoratet Internkontroll/styringssystem

Krysskoplinger til annet regelverk

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

6.4 Sikkerhetsinstruks

§

§ 6-4. ***Sikkerhetsinstruks***

Virksomheter som har eller behandler kraftsensitiv informasjon skal utarbeide og praktisere en sikkerhetsinstruks som sikrer at kravene til informasjonssikkerhet ivaretas. Sikkerhetsinstruksen skal beskrive hvilke system, rutiner og tiltak som er iverksatt for å etterleve kravene til informasjonssikkerhet, herunder krav til beskyttelse, avskjerming og tilgangskontroll.

Sikkerhetsinstruksen skal omfatte informasjon til ansatte og andre rettmessige brukere om taushetsplikten etter energilovens § 9-3 annet ledd og stille krav til undertegning av taushetserklæring. Sikkerhetsinstruksen skal også omfatte informasjon om at taushetsplikten medfører at kraftsensitiv informasjon ikke skal offentliggjøres.

Ordforklaring

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

Hvordan oppfylle kravet

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

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

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

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

Sikkerhetsinstruksen kan bestå av ett eller flere dokumenter.

En brukerinstruks *bør* dekke følgende

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

Maler

Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se NVE maler

NVEs mal for taushetserklæring på norsk og engelsk se NVE maler

Standarder

- NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav

Veiledere

- Digitaliseringsdirektoratet Internkontroll/styringssystem

Krysskoplinger til annet regelverk

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

6.5 Anskaffelser

§

§ 6-5. ***Anskaffelser***

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

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

Plikten til å påse innebærer at det skal iverksettes system og rutiner for å undersøke, og om nødvendig, følge opp at reglene om informasjonssikkerhet og taushetsplikt etterleves.
Bestemmelsene i første og annet ledd gjelder tilsvarende når KBO-enheter setter ut oppdrag for prosjektering, installering, vedlikehold og feilretting av driftskontrollsystemet.

Ordforklaring

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

Hvordan oppfylle kravet?

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

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

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

Eksempel: Leverandør går konkurs

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

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

Eksempel: Leverandørrevisjon

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

Maler

Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se NVE maler

NVEs mal for taushetserklæring på norsk og engelsk se NVE maler

Standarder

NS-EN ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet - Krav

Veiledere

Digitaliseringsdirektoratet Internkontroll/styringssystem

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (norsk)

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (engelsk)

Krysskoplinger til annet regelverk

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

6.6 Begrenset anbudsinnbydelse

§

§ 6-6. ***Begrenset anbudsinnbydelse***

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

Forståelsen av begrenset anbudsinnbydelse bygger på anskaffelsesregelverket.

Ordforklaring

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

Hvordan oppfylle kravet?

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

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

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

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

1. KBO-enheten *må* vurdere om anbudsdokumentene inneholder sikkerhetsgradert eller kraftsensitiv informasjon.
   Virksomheter som ikke er underlagt *sikkerhetsloven* og som ikke har mottatt sikkerhetsgradert informasjon (merket) fra andre virksomheter underlagt *sikkerhetsloven*, skal normalt ikke være i besittelse av sikkerhetsgradert informasjon. Sikkerhetsgradert informasjon skal være tydelig merket i henhold til *sikkerhetslovens* bestemmelser.

2. Hvis anbudsdokumentene inneholder kraftsensitiv eller sikkerhetsgradert informasjon, må KBO-enheten velge begrenset anbudsinnbydelse. Dette betyr at det kun er leverandører som er prekvalifisert og har inngått sikkerhetsavtale med KBO-enheten som får tilsendt anbudsdokumentene.

Eksempel: Begrenset anbudsinnbydelse

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

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

Maler

Informasjonssikkerhetsavtale NVE-avtale mal på norsk og engelsk se NVE maler

NVEs mal for taushetserklæring på norsk og engelsk se NVE maler

Standarder

Veiledere

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (norsk)

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (engelsk)

Veiledning til reglene om offentlige anskaffelser (anskaffelsesforskriften)

Begrenset anbudskonkurranse, Regjeringen 2017

Veiledning i handtering og beskyttelse av sikkerhetsgradert informasjon

Krysskoplinger til annet regelverk

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

6.7. Personkontroll

OBS! Denne paragrafen blir endret ved at hjemmel for politiattest blir forskriftsfestet.

§ 6-7.Personkontroll

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

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

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

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

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

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

Ordforklaringer

Bakgrunnssjekk	Bakgrunnssjekk er prosessen med å innhente, sammenligne og dokumentere informasjon om en person for å bekrefte eller avkrefte det personen selv opplyser. Bakgrunnssjekk består av identitetskontroll, verifisering av utdanning og arbeidserfaring, søk i adresseregistre og andre åpne kilder, sjekk av næringsinteresser og eventuelt kredittsjekk. Full bakgrunnssjekk vil si at alle ovennevnte elementer inngår, også kredittsjekk

Egnethetsvurdering	Helhetsvurdering av om en person er egnet for tilsetting eller tilgang, basert på funn fra bakgrunnssjekken
Kredittsjekk	Kontroll og vurdering av kredittverdigheten og betalingsevnen for en person. Kredittsjekk er en tjeneste som selges av kredittopplysningsbyråer, og er det samme som kredittvurdering.

Hvordan oppfylle kravet

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

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

KBO-enheter kan kreve at personer som skal få tilgang til anlegg, system eller annet i klasse 2 og 3, skal fremlegge kredittsjekk. Dette forutsetter at det er gjennomført en risikovurdering som viser at det ikke finnes andre egnede sikkerhetstiltak. Personer som har sperret muligheten for kredittsjekk, må i så fall åpne for dette.

Dersom KBO-enheten etter en risikovurdering av stillingens oppgaver finner det nødvendig med bruk av kredittsjekk, bør det opplyses om dette i utlysningen. Personkontroll med bruk av kredittsjekk kan også komme til anvendelse på egne ansatte som skifter jobb og går over til en stilling der risikovurderingen tilsier at det er nødvendig med kredittsjekk. Det må være en *annen stilling* og ikke bare endring av stillingsinnhold.

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

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

Eksempel: Personkontroll av ansatte

Kraftkonsernet AS skal ansette en ny medarbeider i en stilling med stort budsjettansvar. Medarbeideren vil få tilgang til anlegg i klasse 2 og 3. Bakgrunnssjekk av nyansatte innebærer for eksempel kontroll av identitet, framvisning av originalvitnemål, verifikasjon av kompetanse og erfaring gjennom intervju og referansesjekk. I tillegg kan Kraftkonsernet AS på bakgrunn av resultatet av risikovurdering gjennomføre kredittsjekk.

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

Kraftkonsernet AS skal også ansatte en lærling som skal jobbe i anlegg i klasse 2 og 3. Han skal ikke jobbe på driftssentralen. I dette tilfellet skal Kraftkonsernet gjennomføre bakgrunnssjekk før ansettelse. Basert på risikovurderingen de gjør, kan de eventuelt gjennomføre kredittsjekk.

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

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

Veiledere

Sikkerhet ved ansettelsesforhold, før, under og ved avvikling, utgitt av Politiets sikkerhetstjeneste, Nasjonal sikkerhetsmyndighet, Politiet og Næringslivets Sikkerhetsråd

Kredittvurdering, Datatilsynet

6.8 Sikkerhetskopier

§

§ 6-8. ***Sikkerhetskopier***

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

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

Hvordan oppfylle kravet

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

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

Annet ledd handler om beredskap for manuell drift. Papirkopikravet gjelder energisystemet. Formålet er å sikre at virksomheten evner å reparere feil i nettet og få gjenopprettet energiforsyningen. Virksomheten må

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

Eksempel: Sikkerhetskopier av driftskontrollsystemet

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

Denne meldingen gikk ut på SMS til alle ansatte i Kraftkonsernet AS. Økonomisystemet var blant de systemene som ble rammet. Angriperen ville ha betalt i kryptovaluta. Beredskapsplanene fantes heldigvis i sikkerhetskopi på andre datamedia og på papir, sikret og adskilt fra de systemene som var rammet. Kraftkonsernet AS hadde tidligere i år testet at systemet kunne gjenopprettes med sikkerhetskopien. Å betale utpressingspenger er sterkt frarådet, og det ble heller ikke gjort. Beskyttet og testet sikkerhetskopi er derfor en god forebyggende sikring mot følgene av slike angrep.

Virksomheten *bør*

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

Veileder

NSM og KRIPOS, 2020, Løsepengevirus temarapport

Standarder

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

Krysskoplinger til annet regelverk

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

6.9 Digitale informasjonssystemer

§

§ 6-9. *Digitale informasjonssystemer*

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

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

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

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

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

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

d. Håndtere og gjenopprette
Virksomheter skal håndtere uønskede hendelser i sine digitale informasjonssystemer og

gjenopprette normaltilstand uten ugrunnet opphold

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

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

Ordforklaring

Digitale informasjonssystemer	Samlebetegnelse for informasjons- og kommunikasjonsteknologi som en virksomhet anvender til operasjonelle og administrative formål. Systemer for generering, samling, lagring, behandling, forvaltning og formidling av data og informasjon, inkludert kommunikasjon og samhandling. Informasjonssystemer kan avgrenses mot styrings-/kontrollsystemer
Konfidensialitet, integritet og tilgjengelighet	De tre klassiske målene for informasjonssikkerhet. Konfidensialitet betyr beskyttelse av informasjon mot innsyn fra uautoriserte personer eller prosesser. Integritet betyr beskyttelse av informasjon mot utilsiktet eller uautorisert endring. Tilgjengelighet betyr tilgang for rettmessige brukere.
Verdi	Med verdi menes virksomhetens leveranser av for eksempel elektrisk energi og fjernvarme, tjenester og produkter. Verdier er også anleggsmidler og informasjon inklusive intellektuelle rettigheter. Listen er ikke prioritert eller uttømmende.
Sikringstiltak	Tiltak for å redusere risiko forbundet med uønskede handlinger
Risikovurdering	Se § 2-3
Sektorvist responsmiljø	Se § 3-6
Uønsket hendelse	Uønskede hendelser omfatter både tilsiktede handlinger og utilsiktede hendelser. Begge deler kan påvirke sikkerhetsverdiene konfidensialitet, integritet og tilgjengelighet. Uønskede hendelser kan gi opphav til ekstraordinære situasjoner.
Hendelseshåndtering	Aktiviteter med formål om å stanse eller begrense skade av uønskede hendelser på berørte IKT-systemer og nettverksressurser, og deretter gjenopprette sikker tilstand.

Tjenesteutsetting	Ekstern utførelse av basisdrift, applikasjonsdrift eller applikasjonsforvaltningmed en tjenesteleverandør. Tjenesteutsetting (outsourcing), utkontraktering og konkurranseutsetting er likeverdige betegnelser
Sikkerhetsrevisjon	Virksomhetens interne og eksterne kontroll av eget sikkerhetsarbeid.

Hvordan oppfylle kravet

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

Internasjonale standarder og veiledning for ytterligere kunnskap

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

Grunnprinsippene forteller hva du må gjøre, men ikke hvordan. Hvert grunnprinsipp beskriver en kontinuerlig aktivitet som må gjennomføres og vurderes i hele systemets levetid, fra planlegging og etablering til avhending. Flere av grunnprinsippene bygger på hverandre, og enkelte er en forutsetning for at andre skal kunne gjennomføres effektivt. I sum inkluderer grunnprinsippene bredden av sikringstiltak som består av barrierer, deteksjon, verifikasjon og reaksjon for å etablere god sikkerhet i dybden.

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

For større virksomheter kommer i praksis alle grunnprinsippene under de ulike hovedkategoriene til anvendelse. Nedenfor følger en gjennomgang av *kravene* i bokstav a til f.

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

a. *Identifisere og dokumentere*

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

Aktiviteten er grunnlaget for effektiv innføring av de øvrige kravene. Hensikten er å forstå virksomhetens leveranser og tjenester, få oversikt over hvilke teknologiske ressurser som bør sikres, og de roller og brukere virksomheten består av. I kravet til å identifisere og dokumentere inngår følgende grunnprinsipper

- 1.1 kartlegg styringsstrukturer, leveranser og understøttende systemer
- 1.2 1kartlegg enheter (inventar) og programvare
- 1.3 kartlegg brukere og behov for tilgang

NVE anbefaler i tillegg at normal nettverkstrafikk kartlegges.

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

Store virksomheter og virksomheter med klasse 2 og klasse 3 driftskontrollsystem bør iverksette samtlige grunnprinsipper og tilhørende tiltak.

b. *Risikovurdering*

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

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

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

Eksempel: Enkel risikovurdering av mindre endring i IT-systemet

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

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

Hva er årsakene til at dette IT- systemet eller IT-tjenesten blir utilgjengelig?
Det kan være mange årsaker med ulik grad av sannsynlighet: Overbelastning av

datatrafikk, infeksjon med kryptoskadevare, ordinær oppdatering av programvare som fører til at kommunikasjon med annen IT-tjeneste ikke fungerer, lisensen har gått ut, strømbrudd, brudd på kommunikasjonslinjer utenfor virksomheten, med flere.

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

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

Om ikke hendelsen kan unngås, hva er konsekvensene for virksomheten? Hvordan kan konsekvensen reduseres? Beredskapsplan og innsatsplaner? Forberedte tiltak som beskyttet og testet sikkerhetskopi? Eller er konsekvensen minimal og kan håndteres av IT-drift dersom den inntreffer?

c. Sikre og oppdage

Virksomheten skal sikre sine digitale informasjonssystem for å motstå eller begrense skaden fra uønskede hendelser. Krav til sikring henger sammen med informasjonsverdi, for eksempel kraftsensitiv informasjon (se. kbf § 6-2), bedriftshemmeligheter, personopplysninger (se *personopplysningsloven*) eller gradert informasjon (se. *sikkerhetsloven*). Annen informasjon vil være åpen informasjon.

I kravet til å sikre inngår følgende grunnprinsipper

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

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

- blokkere kjøring av ikke-autoriserte programmer
- oppgradere program- og maskinvare
- installere sikkerhetsoppdateringer fortløpende
- begrense tildelingen av administratorrettigheter og logge endringer

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

I kravet til å oppdage inngår følgende grunnprinsipper

- 3.1 oppdag og fjern kjente sårbarheter og trusler
- 3.2 etabler sikkerhetsovervåkning

- 3.3 analyser data fra sikkerhetsovervåkning
- 3.4 gjennomfør inntrengningstester

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

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

Eksempel; Varsling av datainnbrudd

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

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

d. Håndtere og gjenopprette

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

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

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

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

Eksempel: Rapportering av hendelse til NVE

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

e. Tjenesteutsetting

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

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

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

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

IT-industrien er global og benytter underleverandører spredt over hele verden. Virksomheter som planlegger tjenesteutsetting, har derfor behov for å vurdere landrisiko for å sørge for at sikkerhetsnivået opprettholdes. Garantikassen for eksportkreditt (GIEK) har en nettside med samlet vurdering av landrisiko for alle land i verden, og NSM har utarbeidet en veileder for landrisikovurdering. For tjenesteutsetting av IKT-systemer som behandler kraftsensitiv informasjon (se. § 6-2), gjelder særlige hensyn for å sikre at taushetsplikten ivaretas. Se også NVEs sjekkliste for IKT-sikkerhet og NSMs veileder for tjenesteutsetting. Aktuelle leverandører bør være sertifisert i henhold til én eller flere internasjonalt anerkjente sikkerhetsstandarder. Eksempler på slike er NIST Cyber Security Framework og ISO/IEC 27000-serien. I slike tilfeller bør virksomheten be om å få se tredjeparts revisjonsrapport eller sertifiseringsbevis.

Følgende arbeidsoppgaver inngår ved tjenesteutsetting

- dokumentere eksisterende system (se. §6-9 a) og organisasjonens IKT-sikkerhetskompetanse
- gjennomføre behovsanalyse
- vurdere forretningsmodeller for IKT-drift og spesifisere krav til leveranse og leverandør
- prekvalifisere leverandører, utlyse anbudskonkurranse og gjennomføre eventuelle forhandlingsmøter
- velge kvalifisert leverandør, gjennomføre kontraktsforhandlinger og inngå kontrakt med kvalifisert(e) leverandør(er)

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

Eksempel: Tjenesteutsetting

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

f. Sikkerhetsrevisjon

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

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

Veiledere

NIST Guide for Conducting Risk Assessment

NSM Grunnprinsipper i sikkerhetsstyring

Digdir Helhetlig styring og kontroll av informasjonssikkerhet

NSM grunnprinsipper for IKT-sikkerhet 2.0

Kvalitetsordning for bruk av leverandørar av tenester for handtering av IKT-hendingar, NSM

Anbefaling om landrisikovurdering ved tjenesteutsetting, NSM (2018)

Garantikassen for eksportkreditt – landrisikovurdering

Sikkerhetsfaglige anbefalinger ved tjenesteutsetting. En utdyping av området Beslutt leveransemodell i NSMs grunnprinsipper for IKT-sikkerhet

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (norsk)

Sjekkliste for IKT-sikkerhet i anskaffelser og tjenesteutsetting i norsk kraftforsyning (engelsk)

Metode for å finne kraftsensitiv informasjon på internett

NSM veiledning (2017) for sikker sletting av data

Digdir_Veileder for testing av etterlevelse av sikkerhetsstandarder

Tiltak mot skadevare og løsepengevirus, NSM (2021)

CIS Benchmarks - konfigurasjonsråd for mange produkter

Sikkerhetsveileder for kraftsensitiv informasjon i skytjenester, FSK (november 2021).

Standarder

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

Krysskoplinger til annet regelverk

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

6.10 Beskyttelse av brytefunksjonalitet i AMS

§

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

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

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

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

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

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

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

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

Ordforklaringer

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

Adgangskontrollert sone	En adgangskontrollert sone (eller område) er et avgrenset og fysisk sikret rom, del av bygning eller bygning med styrt og kontrollert adgang. Virksomheten skal kunne gjøre rede for hvem som er og har vært inne i sonen.
Fjerntilgang	Tilgang til IKT-system fra en fysisk lokalitet utenfor anlegget der IKT-systemets maskinvare befinner seg.
Fjernstyring	Styring som skjer over en geografisk avstand.
Kontrollordninger	Tekniske sikkerhetstiltak, sikkerhetsmekanismer og prosedyrer.

Hvordan oppfylle kravet

Bestemmelsen gjelder for nettselskap som har AMS med brytefunksjonalitet.

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

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

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

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

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

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

Dersom nettselskapet har behov for å gi leverandører utenfor EFTA, EU eller NATO tilgang til AMS, må selskapet gjøre en landrisikovurdering og iverksette nødvendige sikringstiltak. Se punkt § 6-10 e. Leverandører med fjerntilgang til brytefunksjonaliteten må til enhver tid være under oppsyn av kvalifisert personell fra nettselskapet eller kvalifisert personell fra en leverandør som er lokalisert i land som er medlem i EFTA, EU eller NATO. Med oppsyn menes kontinuerlig observasjon. Med kvalifisert personell menes personell med tilstrekkelig kompetanse til å forstå arbeidsoperasjonen som blir gjennomført.

Eksempel: AMS-drift fra utlandet

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

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

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

Aktuelle kontrollordninger kan være

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

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

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

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

Ingen som får kontroll over en måler, og som kan lese av innholdet i den, skal alene kunne bruke kontrollen og/eller informasjonen til å endre innstillingene i andre AMS-målere. Hver måler må derfor ha innebygget sikkerhetsløsning som forhindrer at brytefunksjonaliteten blir misbrukt og at for eksempel skadevare forplanter seg fra en måler til en annen.

Veiledere

Veileder til sikkerhet i avanserte måle- og styringssystem, NVE-rapport 7:2012

NIST Guidelines for Smart Grid Cybersecurity

Krysskoplinger til annet regelverk

- § 6-9 Digitale informasjonssystemer
- Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. se § 1-3

Veiledere

Veileder til sikkerhet i avanserte måle- og styringssystem, NVE-rapport 7:2012

NIST Guidelines for Smart Grid Cybersecurity

Krysskoplinger til annet regelverk

- § 2-10 Internkontrollsystem
- § 5-1 Sikringsplikt
- § 6-9 Digitale informasjonssystemer
- Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv. se § 1-3