Forskrift om objektsikkerhet

Fastsatt ved kgl. res. xx. måned 200x med hjemmel i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) § 17 andre ledd. Fremmet av Forsvarsdepartementet.

Kapittel 1. Alminnelige bestemmelser

§ 1-1. Formål og virkeområde

Forskriften har samme formål og virkeområde som sikkerhetsloven.

§ 1-2. Forkortelser

Nasjonal sikkerhetsmyndighet er i denne forskrift forkortet til NSM.

Kapittel 2. Utvelgelse og klassifisering av skjermingsverdige objekter

§ 2-1. Utpeking av skjermingsverdige objekter

Hvert enkelt departement utpeker skjermingsverdige objekter innen sitt myndighetsområde.

Virksomheten skal overfor vedkommende fagdepartement levere en dokumentert skadevurdering over hvilke objekter som kan være skjermingsverdige.

Der det finnes tilsynsorgan for sektoren, kan disse foreslå skjermingsverdige objekter uavhengig av objekteiers forslag. NSM kan også foreslå skjermingsverdige objekter for departementene.

Utvelgelsen skal ikke skje i større utstrekning enn nødvendig.

Dersom et objekt er avhengig av andre objekter for å kunne fungere etter sin hensikt, skal dette meddeles virksomhet som rår over det understøttende objekt. I meddelelsen skal avhengighetsgrad og skadefølger beskrives slik at dette kan inngå i vurderingsgrunnlaget ved klassifisering av det understøttende objekt jf. § 2-2.

Dersom et objekt foreslås som skjermingsverdig hos en virksomhet som ikke er underlagt sikkerhetsloven, skal det departement som har ansvar for vedkommende sektor ta initiativ til å bringe saken inn for Forsvarsdepartementet.

§ 2-2. Klassifiseringen

Vedkommende departement skal fastsette klassifiseringsgrad for objekter innen sitt myndighetsområde.

Klassifisering av skjermingsverdige objekter skal skje etter en vurdering slik det er beskrevet i sikkerhetsloven § 17a. Det skal også tas hensyn til følgende:

a. Det skal ikke brukes høyere klassifiseringsgrad enn nødvendig.

b. Bare skjermingsverdige deler av objektet skal omfattes av klassifiseringen, og objektet kan inndeles i forskjellige klassifiseringsgrader.

Ved klassifiseringen skal det tas hensyn til objektets betydning for andre objekter.

§ 2-3. Omklassifisering

Ved endring av forhold som er relevante for skadevurderingen av objektet i henhold til sikkerhetslovens § 17, skal vedkommende fagdepartement foreta en ny skadevurdering og eventuelt en omklassifisering.

Omklassifisering kan foretas for å gi et objekt høyere (oppklassifisering) eller lavere (nedklassifisering) klassifiseringsgrad eller for å avklassifisere objektet. Omklassifisering kan gjelde hele objektet eller kun deler av det.

Et avklassifisert objekt regnes ikke som skjermingsverdig objekt etter sikkerhetsloven.

§ 2-4. Registrering og koordinering

De enkelte departementer skal føre register over skjermingsverdige objekter og klassifiseringen av disse innen eget myndighetsområde.

Alle skjermingsverdige objekter skal meldes til NSM med angivelse av klassifiseringsgrad. Ved omklassifisering etter §2-3, skal endringer i tidligere foretatt klassifisering meldes til NSM.

Opplysning om at et objekt er sikkerhetsklassifisert er ugradert. Opplysning om hvilken klassifiseringsgrad et skjermingsverdig objekt har, skal sikkerhetsgraderes minst BEGRENSET. En oversikt over samtlige eller større antall av skjermingsverdige objekter med angivelse av klassifisering, skal sikkerhetsgraderes minst KONFIDENSIELT.

NSM skal i samarbeid med fagdepartementene ivareta nødvendig koordinering, slik at det blir tatt hensyn til tverrsektoriell avhengighet ved utvelgelse og klassifisering.

Kapittel 3. Beskyttelse av skjermingsverdige objekter

§ 3-1. Generelle krav til beskyttelsen

Sikkerhetstiltakene som skal implementeres etter sikkerhetslovens § 17 b skal planlegges, gjennomføres og vedlikeholdes som permanent grunnsikring for objektene. Virksomheten skal også planlegge for og gjennomføre påbygging av grunnsikringen ved økt risiko, jf forskrift om sikkerhetsadministrasjon § 3-4.

Grunnsikringen skal oppfylle kravene innen den aktuelle klassifiseringsgrad, jf. sikkerhetslovens § 17 b. Tiltakene skal bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som er tilpasset det enkelte objekt.

Barrierer skal forhindre eller redusere muligheten for at sikkerhetstruende hendelser kan inntreffe. Barrierene kan være av fysisk, elektronisk eller administrativ art.

Deteksjonstiltak skal etableres for å avdekke hvorvidt etablerte barrierer brytes eller blir forsøkt brutt fra innsiden eller utsiden.

Verifikasjonstiltak skal ta sikte på å etablere en situasjonsforståelse hvis en sikkerhetstruende hendelse inntreffer. Tiltakene skal ha som formål å kunne identifisere og avdekke aktører, identifisere skadeomfang og identifisere de midler som eventuelt er anvendt av en aktør.

Reaksjonstiltak skal sikre opprettholdelse av objektets funksjonalitet ved en sikkerhetstruende hendelse, eller sikre forutsetninger for gjenopprettelse av funksjonalitet etter en slik hendelse. Aktuelle reaksjonstiltak skal være forberedt som en del av grunnsikringen.

Dersom grunnsikring etter sikkerhetsloven § 17b ikke kan gjennomføres uten at dette kommer i konflikt med de informasjonssikkerhetstiltak som virksomheten skal implementere etter sikkerhetslovens kapittel 4, skal det etableres tilpassede sikkerhetstiltak etter en risikovurdering hvor de ulike sikkerhetshensyn avveies. Dersom slike tilpassede sikkerhetstiltak fraviker bestemmelser gitt i eller i medhold av sikkerhetslovens kapittel 4, skal tiltakene forelegges NSM for godkjenning før de gjennomføres.

Som grunnlag for fastsettelse av sikkerhetstiltak skal objekteier foreta risikovurdering og sikkerhetsrevisjon etter forskrift om sikkerhetsadministrasjon kapittel 4.

§ 3-2. Tiltak mot etterretningsaktivitet

Objekteier skal beskytte objektet mot informasjonsinnhenting som kan ha til hensikt å forberede sabotasje eller terrorhandling. Sikkerhetstiltakene skal ta sikte på i nødvendig grad å redusere muligheten for uønsket innhenting av opplysninger om funksjoner, betydning, kapasitet, sårbarhet og sikkerhetstiltak knyttet til objektet.

Når informasjon om et skjermingsverdig objekt må beskyttes av sikkerhetsmessige grunner, skal den sikkerhetsgraderes etter sitt innhold, og beskyttes etter bestemmelsene gitt i og i medhold av sikkerhetslovens kapittel 4.

§ 3-3. Tilrettelegging for beskyttelse av IKT-infrastruktur

Dersom tilknytning til internett utgjør en sårbarhet for sikkerheten til et skjermingsverdig objekt, kan NSM i samråd med virksomheten og vedkommende departement bestemme at objekteier skal være tilknyttet et sentralt system for varsling av koordinerte angrep via internett. NSM kan gi nærmere bestemmelser om hvordan tilknytningen skal settes opp og forvaltes.

§ 3-4. Tiltak mot elektromagnetisk puls og høyfrekvente mikrobølger

Ved gjennomføring av risikovurdering og sikkerhetsrevisjon etter forskrift om informasjonssikkerhet kapittel 4 skal behovet for å beskytte elektroniske systemer mot elektromagnetisk puls (EMP) og høyfrekvente mikrobølger (HPM) vurderes.

§ 3-5. Tilrettelegging for bruk av sikringsstyrker

Objekteier eller den som råder over et skjermingsverdig objekt utvalgt i henhold til bestemmelsene i denne forskriften, plikter å legge til rette for at sikringsstyrker kan forberede, øve og gjennomføre tiltak på og ved objektet for å beskytte dette.

§ 3-6. Sikkerhetsklarering og autorisasjon

Vedkommende departement kan bestemme at enhver som skal gis permanent adgang til skjermingsverdig objekt klassifisert som KRITISK eller MEGET KRITISK skal være autorisert og sikkerhetsklarert før slik adgang gis. Sikkerhetsklarering skal ikke foretas der dette ikke anses som et egnet virkemiddel. Dersom objekteier mener det bør stilles krav til sikkerhetsklarering for person som skal ha permanent adgang til objektet, må dette nærmere begrunnes.

Dersom det kreves sikkerhetsklarering, skal det for adgang til objekt eller del av objekt klassifisert KRITISK, kreves sikkerhetsklarering for KONFIDENSIELT eller høyere, og for objekter klassifisert MEGET KRITISK kreves sikkerhetsklarering for HEMMELIG eller høyere.

Ved sikkerhetsklarering og autorisasjon gjelder bestemmelsene gitt i og i medhold av sikkerhetslovens kapittel 6. NSM skal informeres om hvilke skjermingsverdige objekter det kreves sikkerhetsklarering for.

Besøkende som ledsages av autorisert representant behøver ikke sikkerhetsklareres.

Før besøkende gis adgang til skjermingsverdig objekt eller del av objekt klassifisert som KRITISK eller MEGET KRITISK, skal det forsikres om at deres identitet er korrekt. Alle besøkende skal registreres, og registreringen skal oppbevares i minimum fem år. For representanter for annen stat, internasjonal organisasjon eller utenlandsk rettssubjekt skal det også forsikres om at disse faktisk representerer vedkommende stat, organisasjon eller utenlandske rettssubjekt.

Det enkelte departement kan innen den sektor departementet forvalter fatte beslutning om nærmere sikkerhetsprosedyrer for godkjenning og gjennomføring av besøk fra representanter for fremmede stater, internasjonale organisasjoner og utenlandske rettssubjekter.

Kapittel 4. Administrative bestemmelser

§ 4-1. Iverksettelse av tiltak – kostnader og dispensasjon

Den enkelte virksomhet skal dekke egne kostnader som følge av tiltak eller pålegg i eller i medhold av sikkerhetslovens kapittel 5 og denne forskrift.

Virksomheten kan i særlige tilfeller søke om dispensasjon fra sikkerhetstiltak der dette anses forsvarlig. Slik søknad avgjøres av vedkommende fagdepartement, om nødvendig etter konsultasjon med NSM.

§ 4-2. Internkontroll

Objekteier skal utføre internkontrolltiltak i samsvar med forskrift om sikkerhetsadministrasjon.

§ 4-3. Tilsyn og påleggskompetanse

NSM skal føre tilsyn med at utvelgelse og klassifisering av skjermingsverdige objekter skjer i henhold til sikkerhetsloven og denne forskrift, og eventuelt gi nødvendige pålegg i samsvar med sikkerhetslovens § 9 litra c.

NSM skal føre overordnet tilsyn med at sikkerhetstiltak implementeres i henhold til denne forskriften. Der det finnes tilsynsorganer med ansvar for forebyggende sikkerhet i en sektor, skal primært dette tilsynsorganet føre tilsyn med at sikkerhetstiltakene i de enkelte virksomhetene tilfredsstiller de funksjonelle kravene i sikkerhetsloven kap 5 og denne forskrift.

Kapittel 5. Sluttbestemmelser

§ 5-1. Ikrafttredelse

Denne forskriften trer i kraft xx.xx.xxxx.

§ 5-2. Overgangsbestemmelser

Første gangs fastsettelse av sikkerhetsklassifisering, jf. kapittel 2, vurdering av tiltak mot etterretningstrussel i forbindelse med klassifisering, jf. § 3-2 andre ledd, skal skje senest ett år etter ikrafttredelsen.

Gjennomføring av sikkerhetstiltak i samsvar med kapittel 3 på bakgrunn av fastsatt sikkerhetsklassifisering og tilrettelegging for sikringsstyrker i samsvar med § 4-2, skal skje så raskt som mulig og senest to år etter ikrafttredelsen. Gjennomføringen og tilretteleggingen kan etter søknad til NSM utsettes ytterligere med inntil ett år.

Opprettelse av internkontrollsystem, jf. § 4-2, skal skje senest tre år etter ikrafttredelsen.

Forslag til endringer i forskrift om sikkerhetsadministrasjon:

I forskrift av 29. juni 2001 nr. 723 om sikkerhetsadministrasjon gjøres følgende endringer (endringer i kursiv):

§ 1-1, annet ledd skal lyde:

Forskriften gjelder den enkelte virksomhets sikkerhetsadministrasjon innen og på tvers av fagområdene informasjonssikkerhet, *objektsikkerhet*, personellsikkerhet og sikkerhetsgraderte anskaffelser.

§ 1-2 skal lyde:

I forskriften forstås med:

1. **Sikkerhetsadministrasjon;** internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt i og i medhold av sikkerhetsloven.
2. **Sikkerhetstruende hendelse;** sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon *eller objekt* og grove sikkerhetsbrudd.
3. **Kompromittering**; tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon, herunder uønsket avhending, modifisering eller ødeleggelse, *eller tap eller mistanke om tap av funksjonalitet eller rettmessig kontroll med skjermingsverdig objekt.*
4. **Sikkerhetsbrudd;** brudd på bestemmelse om sikkerhetstiltak gitt i sikkerhetsloven eller forskrifter til sikkerhetsloven.
5. **Fagområder;** informasjonssikkerhet, *objektsikkerhet,* personellsikkerhet og sikkerhetsgraderte anskaffelser. Informasjonssikkerhet innen den enkelte virksomhet består av blant annet dokumentsikkerhet, informasjonssystemsikkerhet, fysisk sikring og administrativ kryptosikkerhet.

§ 2-6, første ledd skal lyde:

Ved større prosjekter eller anskaffelser som involverer sikkerhetsgradert informasjon *eller skjermingsverdig objekt* skal det utpekes en prosjektsikkerhetsleder.

§ 2-6, tredje ledd skal lyde:

Dersom to eller flere virksomheter er tilkoblet et felles informasjonssystem, *eller sammen råder over eller eier skjermingsverdig objekt* påhviler ansvaret for sikkerheten i informasjonssystemet *eller for objektet* felles overordnet virksomhet eller den denne utpeker, eller den som er utpekt i skriftlig avtale inngått mellom virksomhetene. I avtalen skal det fremgå hvilken sikkerhetsgrad informasjonssystemene er sikkerhetsgodkjent for, og hvilke sammenkoblinger med andre informasjonssystemer som tillates, *eller hvilken klassifiseringsgrad objektet innehar.*

§ 3-3 skal lyde:

Virksomhet med skjermingsverdig informasjon *eller objekt* skal ha et ajourført grunnlagsdokument for sikkerhet. Grunnlagsdokumentet skal identifisere grunnleggende forutsetninger for virksomhetens håndtering av skjermingsverdig informasjon *eller objekt,* herunder:

1. sikkerhetsorganisasjonen og dens myndighet,
2. sikkerhetsmessig inndeling i fysiske områder ved virksomheten, og hvor sikkerhetsgradert informasjon tillates behandlet og oppbevart med angivelse av høyeste sikkerhetsgrad, *og hvor skjermingsverdig objekt befinner seg,*
3. hvilke informasjonssystemer, herunder kryptosystemer, som håndterer sikkerhetsgradert informasjon, med angivelse av hvilken sikkerhetsgrad hvert system er sikkerhetsgodkjent for og i hvilke fysiske områder det enkelte system er plassert,
4. oversikt over kommunikasjon av sikkerhetsgradert informasjon som er etablert internt i virksomheten og mot andre virksomheter,
5. hvem som har behov for tilgang til hvilken type skjermingsverdig informasjon med tilhørende informasjonssystemer, *eller adgang til skjermingsverdig objekt* og
6. planer, instrukser og annen dokumentasjon for sikkerhet.

§ 3-4, første ledd skal lyde:

Virksomheten skal utarbeide skriftlige instrukser for rutiner og prosedyrer innenfor aktuelle fagområder. Instruksene skal tilpasses størrelsen og kompleksiteten på virksomheten, herunder virksomhetens sikkerhetsgraderte informasjon *eller klassifiserte objekter* med tilhørende informasjonssystemer og styringssystemer.

§ 4-1 skal lyde:

Virksomhet med skjermingsverdig informasjon *eller objekt* skal utøve risikohåndtering, ved å fastsette og gjennomføre sikkerhetstiltak etter en risikovurdering.

§ 4-2, andre ledd, første punkt, skal lyde:

Den enkelte virksomhet skal foreta kontinuerlige *skriftlige* risikovurderinger med utgangspunkt i grunnlagsdokument for sikkerhet

§ 4-2, fjerde ledd, skal lyde:

Når det foreligger særlige grunner kan NSM bestemme hvilken vurderingsmetode som skal legges til grunn for risikovurderingen.

§ 5-2, nytt annet ledd skal lyde:

Ved kompromittering av objekt klassifisert KRITISK eller høyere skal virksomheten som eier eller råder over objektet utarbeide skadevurdering. Skadevurderingen skal redegjøre for tiltak som kan redusere skaden, og adresseres til berørte virksomheter og andre som kan bidra til skadereduserende tiltak. Kopi av skadevurderingen skal formidles til NSM.

§ 5-5 skal lyde:

Virksomhet som oppdager kompromittering skal rapportere til virksomheten som har tilvirket informasjonen *eller som eier eller råder over objektet*, og andre virksomheter dette har betydning for. Rapporten skal redegjøre for mulig årsak til kompromitteringen og hva som er gjort for å hindre gjentagelse. Dersom forholdet skal rapporteres til NSM, kan kopi av rapportene til NSM benyttes ved rapportering til andre virksomheter.

§ 5-6, første ledd skal lyde:

En virksomhet skal snarest mulig avgi foreløpig rapport til NSM dersom den oppdager:

a. *sikkerhetstruende hendelser, eller*
b. *sikkerhetsbrudd vedrørende informasjon sikkerhetsgradert av utenlandske myndigheter eller internasjonal organisasjon, eller*
c. *kompromittering av klassifiserte objekter.*