Nasjonal sikkerhetsmyndighet

Veiledning

Sist oppdatert: 2010-07-01

Sikkerhetsadministrasjon

Veiledning til bestemmelser om sikkerhetsstyring i sikkerhetsloven med forskrifter.

Dette dokumentet veileder virksomheter som håndterer skjermingsverdig informasjon eller skjermingsverdige objekter og som derfor plikter å utøve forebyggende sikkerhetstjeneste for å håndtere risiko for spionasje, sabotasje eller terrorvirksomhet. Sikkerhetstjenesten må gi nødvendig beskyttelse, gi grunnlag for tillit til denne beskyttelsen og være mulig å kontrollere. Sikkerhetstjenesten må derfor utøves gjennom planlagt og systematisk sikkerhetsadministrasjon i form av et styringssystem for sikkerhet.

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) koordinerer forebyggende sikkerhetstjeneste og kontrollerer sikkerhetstilstanden i virksomheter som håndterer skjermingsverdig informasjon eller skjermingsverdige objekter. NSM utvikler sikkerhetstiltak og -prosedyrer for forebyggende sikkerhet, veileder virksomheter i etablering av forebyggende sikkerhetstjeneste, godkjenner informasjonssystemer for behandling av sikkerhetsgradert informasjon og fører tilsyn med at bestemmelsene i eller i medhold av sikkerhetsloven oppfylles.

Hensikten med veiledningen

Forebyggende sikkerhetstjeneste må utøves gjennom planlagt og systematisk sikkerhetsadministrasjon i form av et styringssystem for sikkerhet. Dette dokumentet veileder virksomheter i utforming, iverksetting og oppfølging av et slikt styringssystem.

Postadresse
Postboks 14
1306 BÆRUM
POSTTERMINAL

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09

Internettadresse
www.nsm.stat.no

Innhold

1 Innledning

1.1 Bakgrunn

Sikkerhetsloven gjelder for virksomheter som behandler skjermingsverdig informasjon eller som råder over skjermingsverdig objekt. Kun virksomheter som er organ for stat eller kommune, leverandør i sikkerhetsgradert anskaffelse eller underlagt sikkerhetsloven gjennom enkeltvedtak kan håndtere skjermingverdig informasjon eller objekt. Disse virksomhetene plikter å utøve forebyggende sikkerhetstjeneste.

Skjermingsverdig informasjon er informasjon som kan skade Norges eller alliertes sikkerhet, forholdet til fremmede makter eller andre vitale sikkerhetsinteresser dersom den blir kjent for uvedkommende. Skjermingsverdig objekt er objekt der redusert funksjonalitet, skade, ødeleggelse eller overtagelse av andre, kan skade Norges selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.

Forebyggende sikkerhetstjeneste er alle aktiviteter og tiltak for å beskytte skjermingsverdig informasjon eller skjermingsverdige objekter mot risiko som følge av spionasje, sabotasje eller terrorvirksomhet. Sikkerhetstjenesten må utøves slik at den gir grunnlag for tillit til beskyttelsen, og slik at den er mulig å kontrollere. Forebyggende sikkerhetstjeneste må derfor utøves gjennom planlagt og systematisk sikkerhetsadministrasjon.

Sikkerhetsadministrasjon er den internkontroll (sikkerhetsstyring) som ligger til grunn for den forebyggende sikkerhetstjenesten og omfatter elementene:

- sikkerhetsledelse
- sikkerhetsorganisering
- sikkerhetstiltak og -prosedyrer
- forholdet til andre virksomheter
- sikkerhetsoppfølging
- sikkerhetsdokumentasjon
- risiko

… organisert i et styringssystem for sikkerhet, slik at den forebyggende sikkerhetstjenesten:

planlegges, gjennomføres, kontrolleres og kontinuerlig forbedres

1.2 Hensikt

Sikkerhetsloven med tilhørende forskrifter (regelverket) har en rekke bestemmelser om sikkerhetsstyring. Disse er i første rekke gitt i loven selv og i forskrift om sikkerhetsadministrasjon, men finnes også i forskriftene for øvrig. Oppfyllelse av bestemmelsene hver for seg har liten eller ingen effekt. Kun når bestemmelsene ses i sammenheng er grunnlaget for en fungerende forebyggende sikkerhetstjeneste lagt.

Denne veiledningen knytter regelverkets bestemmelser om sikkerhetsstyring til styringselementene nevnt over. Tilnærmingen synliggjør sammenhenger mellom enkeltbestemmelser og tydeliggjør enkeltbestemmelsers betydning for sikkerhetsstyringen som helhet.

Behovet for forebyggende sikkerhetstjeneste utgjør ofte kun en liten, om enn viktig, del av virksomhetens sikkerhetsbehov. Andre sikkerhetsbehov må også oppfylles eksempelvis knyttet til helse miljø og sikkerhet eller til behandling av personopplysninger. Effektivt fungerende sikkerhetsarbeid forutsetter at forskjellige sikkerhetsbehov ses og løses i sammenheng.

Forebyggende sikkerhetstjeneste vil ikke fungere kun som et vedheng til sikkerhetsarbeidet for øvrig. Sikkerhetstjenesten må integreres i og bli en del av et helhetlig sikkerhetsarbeid. Tilnærmingen i denne veiledningen legger til rette for slik samordning.

1.3 Om veiledningen

Veiledningen beskriver utforming, iverksetting og oppfølging av det styringssystem for sikkerhet som skal danne grunnlaget for den forebyggende sikkerhetstjenesten. I veiledningen beskrives de forskjellige styringselementene sammen med de forhold disse er ment å ivareta.

Veiledningen omhandler i første rekke bestemmelsene om sikkerhetsstyring i sikkerhetsloven og i forskrift om sikkerhetsadministrasjon. Disse er referert til i de enkelte avsnitt. Der det er aktuelt har veiledningen også utgangspunkt i bestemmelser i de øvrige forskriftene. Dette er angitt i de avsnitt det gjelder.

Detaljerte regler for beskyttelse av skjermingsverdige objekter er ennå ikke utarbeidet. Veiledningen omhandler derfor kun sikkerhetslovens bestemmelser om beskyttelse av slike objekter.

Regelverket omfatter en rekke detaljerte bestemmelser om sikkerhetstiltak og -prosedyrer. Korte beskrivelser av de mest sentrale bestemmelser om slike tiltak og prosedyrer fremgår av veiledningens kapittel 4. Mer detaljert informasjon knyttet til bestemmelser om sikkerhetstiltak og -prosedyrer innen forskjellige fagområder er tilgjengelig fra NSM, blant annet i egne veiledninger.

Veiledningen er utformet slik at beskrivelser av de enkelte styringselementene kan leses noen lunde selvstendig. Flere bestemmelser i regelverket er relevante for mer enn ett styringselement. Gjentagelser er følgelig ikke helt til å unngå, men er søkt redusert ved at mest ufyllende veiledning er gitt der bestemmelsen anses mest relevant.

Veiledningen representerer en autoritativ fortolkning av regelverkets bestemmelser om sikkerhetsstyring. Denne er gyldig for de fleste virksomheter i de fleste situasjoner, men representerer kun en fortolkning. Andre fortolkninger kan være mulige og mer hensiktsmessige i en gitt situasjon. Det påhviler da virksomheten å sannsynliggjøre dette. Dersom det oppfattes motstrid mellom veiledningen og regelverket går regelverket foran.

1.4 Referanser

Lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)

Forskrift av 29. juni 2001 nr. 732 om sikkerhetsadministrasjon

Forskrift av 29. juni 2001 nr. 722 om personellsikkerhet

Forskrift av 1. juli 2001 nr. 744 om informasjonssikkerhet

Forskrift av 1. juli 2001 nr. 753 om sikkerhetsgraderte anskaffelser

Lov av 14. april 2000 nr 31 om behandling av personopplysninger (personopplysningsloven)

2 Sikkerhetsledelse

Dette kapittelet gir veiledning i regelverkets bestemmelser om sikkerhetsledelse, det vil si om virksomhetsledelsens[1] rolle i den forebyggende sikkerhetstjenesten. Denne rollen omfatter overordnet ansvar og myndighet ved utforming, iverksetting og oppfølging av sikkerhetstjenesten. I tillegg er virksomhetsledelsen tillagt utøvende ansvar for enkelte sikkerhetsoppgaver.

Virksomhetens leder har det endelige ansvar for utøvelse av forebyggende sikkerhetstjeneste. Dette innebærer også ansvar for oppgaver med sikkerhetsmessig betydning som utføres av andre på virksomhetens vegne, samt ansvar for sikkerhetstjeneste i underlagte virksomheter.

Sikkerhetsledelse er sikkerhetsstyringens viktigste element. Tilstrekkelig og effektiv forebyggende sikkerhetstjeneste er kun mulig med en aktiv og engasjert ledelse.

2.1 Kunnskaper om sikkerhetsloven

Virksomhetsledelsen må kjenne til sikkerhetslovens virkeområde og herunder vite hvem som kan behandle skjermingsverdig informasjon.

Sikkerhetsloven gjelder for forvaltningsorganer, det vil si for organer for stat eller kommune. Loven gjelder også for leverandører i sikkerhetsgraderte anskaffelser. Loven kan gjøres gjeldende for andre gjennom enkeltvedtak. Sikkerhetsloven gjelder delvis for domstolene, men ikke for Stortinget, Riksrevisjonen, Stortingets ombudsmann for forvaltningen eller for andre organer for Stortinget.

Virksomheter må autoriseres for behandling av skjermingsverdig informasjon før slik behandling igangsettes. Autorisasjon gis i samsvar med tjenstlig behov og til og med det graderingsnivå som er nødvendig.

Statens forvaltningsorganer autoriseres av overordnet departement. Kommuner og fylkeskommuner autoriseres av fylkesmannen. Forvaltningsorganer kan autorisere underlagte forvaltningsorgan innen rammene av egen autorisasjon. Anskaffelsesmyndighet autoriserer leverandører i sikkerhetsgraderte anskaffelser. Andre private virksomheter autoriseres av det departement som forvalter den aktuelle sektoren.

sikkerhetsloven § 2 *– om hvem sikkerhetsloven gjelder for*
sikkerhetsloven § 5, 3. ledd *– om virksomhetsledelsens ansvar*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Virksomhetsledelsen må ha kunnskap om sikkerhetslovens formål og om nødvendige avveininger ved etablering av forebyggende sikkerhetstjeneste.

Sikkerhetslovens formål er å motvirke trusler mot Norges selvstendighet og sikkerhet, og mot andre vitale nasjonale sikkerhetsinteresser, gjennom beskyttelse av skjermingsverdig informasjon og skjermingsverdige objekter.

Virkemidler som iverksettes for å oppnå slik beskyttelse kan ikke være mer inngripende enn nødvendig. Ved utøvelse av forebyggende sikkerhetstjeneste må det tas særlig hensyn til den enkeltes rettssikkerhet. Dersom utøvelsen innebærer behandling av personopplysninger må behandlingen skje i samsvar med grunnleggende personvernhensyn:

- behandlingen må ha et klart avgrenset formål og kun omfatte de opplysningene som er nødvendige for å oppnå dette formålet

[1] Bruk av begrepet "virksomhetsledelse" innebærer at det aktuelle forholdet må ivaretas av en eller flere representanter for virksomhetens øverste ledelse. For forhold virksomhetens øverste leder selv må ivareta benyttes begrepet "virksomhetens leder".

- behandlingen må ha et rettsgrunnlag, eksempelvis sikkerhetsloven, andre regelverk eller samtykke fra den det behandles opplysninger om
- opplysningene må være korrekte og oppdaterte nok til at behandlingen gir riktig resultat
- det må gis innsyn i behandlingen og, for dem de omhandler, i personopplysningene, så langt dette er mulig innenfor sikkerhetsbehovet
- personopplysningene må sikres, ikke bare av hensyn til den forebyggende sikkerhetstjenesten, men også i forhold til behovet for personlig integritet og privatlivets fred

sikkerhetsloven § 1 *– sikkerhetslovens formål*
sikkerhetsloven § 5, 3. ledd *– om virksomhetsledelsens ansvar*
sikkerhetsloven § 6 *– om forholdsmessighet ved iverksetting av tiltak*

2.2 Forståelse for risiko

Virksomhetsledelsen må kjenne til hvilken skjermingsverdig informasjon og hvilke skjermingsverdige objekter virksomheten håndterer.

Skjermingsverdig informasjon er informasjon som må beskyttes for å hindre at Norges eller alliertes sikkerhet, forholdet til fremmede makter eller andre vitale sikkerhetsinteresser skades. Beskyttelsesbehovet angis ved sikkerhetsgradering.

Skjermingsverdig objekt er eiendom som må beskyttes for å forhindre at Norges selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser skades. Beskyttelsesbehovet angis ved klassifisering.

sikkerhetsloven § 5, 3. ledd *– om virksomhetsledelsens ansvar*
sikkerhetsloven § 11 *– om sikkerhetsgradering av skjermingsverdig informasjon*
sikkerhetsloven § 17b *– om klassifisering av skjermingsverdig objekt*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Virksomhetsledelsen må kjenne til mulige trusler og sårbarheter overfor sikkerhetsgradert informasjon eller klassifisert objekt.

Kjennskap til trusler og sårbarheter forutsetter oppfatninger om hvordan uønskede hendelser kan forårsakes og hvem trusselaktørene kan være. Slik kunnskap må baseres på informasjon om resultater fra virksomhetens håndtering av uønskede hendelser, fra gjennomføring av sikkerhetsrevisjoner og på informasjon fra eksterne kilder[2].

sikkerhetsloven § 5, 3. ledd *– om virksomhetsledelsens ansvar*
forskrift om sikkerhetsadministrasjon § 4-1 *– om risikohåndtering*
forskrift om sikkerhetsadministrasjon § 4-4 *– om fremleggelse av avvik for virksomhetsledelsen*
forskrift om sikkerhetsadministrasjon § 5-4, 1. ledd *– om rapportering til virksomhetsledelsen*

[2] Eksempelvis Nasjonal sikkerhetsmyndighets Sikkerhetsvarsler og Rapport om sikkerhetstilstanden.

2.3 Etablering av forebyggende sikkerhetstjeneste

Virksomhetsledelsen må etablere en tilfredsstillende forebyggende sikkerhetstjeneste og herunder utpeke en sikkerhetsorganisasjon med tilstrekkelig omfang.

Virksomhetsledelsen må etablere forebyggende sikkerhetstjeneste i samsvar med regelverkets bestemmelser og plikter å avsette nødvendige ressurser, det vil si personell, kompetanse og verktøy, for å ivareta denne sikkerhetstjenesten.

Den forebyggende sikkerhetstjenesten må etableres slik at den gir grunnlag for tillit til at nødvendig beskyttelse er oppnådd og slik at den er mulig å kontrollere. Dette oppnås gjennom etablering av planlagt og systematisk sikkerhetsadministrasjon i form av et styringssystem for sikkerhet.

Den forebyggende sikkerhetstjenesten må etableres slik at ingen enkelpersoner, aktivt eller passivt, alene kan undergrave sikkerheten. Det må derfor være klare skiller mellom utøvende og kontrollerende oppgaver.

Virksomhetens sikkerhetsorganisasjon må omfatte en sikkerhetsleder med stedfortreder, og i tillegg det antall funksjoner og personer som virksomhetens sikkerhetsbehov, omfang og kompleksitet krever.

Den forebyggende sikkerhetstjeneste må, så langt det er praktisk og tjenlig, samordnes med virksomhetens styringssystem for øvrig, herunder må ivaretakelse og kontroll av sikkerhet integreres i øvrige aktiviteter.

sikkerhetsloven § 1 *– om forebyggende sikkerhetstjeneste som gir grunnlag for tillit og muligheter for kontroll*
sikkerhetsloven § 5, 1. og 3. ledd *– om plikt til å utøve forebyggende sikkerhetstjeneste*
forskrift om sikkerhetsadministrasjon § 1-1, 3. ledd *– om samordning av sikkerhetsadministrasjon*
forskrift om sikkerhetsadministrasjon § 2-1 *– om overordnet ansvar og ansvar for ressurstildeling*
forskrift om sikkerhetsadministrasjon § 2-2, 1. ledd *– om integrering i øvrige aktiviteter*
forskrift om sikkerhetsadministrasjon § 2-4 *– om fordeling av oppgaver*
forskrift om sikkerhetsadministrasjon § 2-5, 1. ledd *– om ansvar for utpeking av sikkerhetsorganisasjonen*

Virksomhetsledelsen må sørge for at personellet har den kompetanse som er nødvendig for sikker arbeidsutførelse.

Alle som utfører arbeidsoppgaver med betydning for sikkerhet må ha den kompetanse, det vil si de holdninger, kunnskaper og ferdigheter, som er nødvendig for sikker arbeidsutførelse.

Personellet har plikt til å bidra til forebyggende sikkerhetstjeneste. Virksomhetsledelsen må opplyse om hvordan denne plikten forventes oppfylt. Intern instruks for å ivareta sikkerhet må utarbeides og fordeles til dem den gjelder.

Riktig kompetanse oppnås gjennom informasjon om og veiledning i hvordan forebyggende sikkerhetstjeneste utøves i virksomheten. Motivering og bevisstgjøring av behovet for forebyggende sikkerhetstjeneste må vektlegges i informasjons- og veiledningsarbeidet.

Riktig kompetanse oppnås også gjennom grunnleggende opplæring i sikkerhet og gjennom opplæring tilpasset den enkeltes behov.

sikkerhetsloven § 5, 2. ledd, litra a og b og 3. ledd *– om ansvar for instruks og for opplæring*
forskrift om sikkerhetsadministrasjon § 3-1, 1. ledd *– om ansvar for veiledning*

2.4 Oppfølging av forebyggende sikkerhetstjeneste

Virksomhetsledelsen må kjenne til hvordan den forebyggende sikkerhetstjenesten utøves og fungerer og sørge for nødvendige forbedringer.

Virksomhetsledelsen må forsikre seg om at den forebyggende sikkerhetstjenesten er etablert som besluttet og gir tilfredsstillende sikkerhet som resultat. Kunnskaper om sikkerhetstjenestens utøvelse og funksjon må baseres på informasjon om resultater fra sikkerhetsrevisjoner og på erfaringer fra håndteringen av uønskede hendelser.

Virksomhetsledelsen må minst årlig gjennomgå den forebyggende sikkerhetstjenesten. Ledelsens evaluering må resultere i beslutninger om nødvendige forbedringer av sikkerhetstjenesten.

sikkerhetsloven § 5, 2. ledd, litra c og 3. ledd *– om ansvar for kontroll*
forskrift om sikkerhetsadministrasjon § 4-4, 1. og 2. ledd *– om sikkerhetsrevisjon og ledelsens evaluering*
forskrift om sikkerhetsadministrasjon § 5-4, 1. ledd *– om rapportering av sikkerhetstruende hendelser*

2.5 Den foresattes ansvar

Foresatte i virksomheten har ansvar for sikkerhet innen sitt ansvars- og myndighetsområde.

Foresatte som avdelingssjefer, mellomledere eller lignende har overordnet ansvar for utøvelsen av forebyggende sikkerhetstjeneste innen sitt ansvars- og myndighetsområde. Dette ansvaret utøves gjennom aktiv og engasjert ledelse og forutsetter at den foresatte:

- har kunnskaper om regelverket og om regelverkets betydning for arbeidsutførelsen
- har forståelse for den risiko sikkerhetsgradert informasjon eller klassifisert objekt er utsatt for
- bidrar til utøvelse av forebyggende sikkerhetstjeneste, blant annet gjennom å informere og veilede underordnet personell
- bidrar til oppfølging av forebyggende sikkerhetstjenesten, blant annet ved å sørge for at uønskede hendelser rapporteres og korrigeres

Foresattes ansvar omfatter også ansvar for utførelse av sikkerhetsoppgaver som er overlatt til andre, eksempelvis til private leverandører.

merknad: For store virksomheter lokalisert på flere steder kan det være hensiktsmessig å etablere en mer selvstendig, lokal forebyggende sikkerhetstjeneste for avdeling, tjenestested eller lignende. Den foresattes oppgaver vil da i hovedsak tilsvare oppgavene tillagt virksomhetsledelsen. Foresattes ansvars- og myndighetsutøvelse må likevel skje i samsvar med de overordnede føringer og bestemmelser som gjelder for virksomheten som helhet.

forskrift om sikkerhetsadministrasjon § 2-2 *– om den foresattes ansvar*

2.6 Sikkerhetsoppgaver tillagt virksomhetsledelsen

Virksomhetens leder er ansvarlig for å autorisere personell for tilgang til sikkerhetsgradert informasjon.

Personell må autoriseres for tilgang til sikkerhetsgradert informasjon før slik tilgang gis. Kun personell som har tjenstlig behov for tilgang til sikkerhetsgradert informasjon kan autoriseres.

Det er normalt virksomhetens leder som er autorisasjonsansvarlig. I virksomheter med et stort autorisasjonsbehov kan myndigheten til å gi autorisasjon delegeres.

sikkerhetsloven § 19, 1. og 3. ledd *– om tilgang til skjermingsverdig informasjon*
sikkerhetsloven § 23, 5. ledd *– om ansvar for å gi autorisasjon*
Ytterligere bestemmelser er gitt i ***forskrift om personellsikkerhet.***

Virksomhetsledelsen har utøvende ansvar for enkelte sikkerhetsoppgaver.

Virksomhetsledelsen må særlig sørge for utførelse av sikkerhetsoppgaver som i regelverket er tillagt ledelsen direkte.

Enkelte oppgaver må virksomhetens leder selv utføre:

- utpeke personell som må ha tilgang til personkontrollopplysninger
- autorisere part i forvaltningssak for innsyn i informasjon sikkerhetsgradert BEGRENSET
- dispensere fra krav om oppbevaring av sikkerhetsgradert informasjon i arkiv
- sikkerhetsgodkjenne informasjonssystemer når virksomheten selv er godkjenningsmyndighet
- håndtere henvendelser fra Nasjonal sikkerhetsmyndighet om tekniske sikkerhetsundersøkelser, monitoring eller inntregningstesting

Enkelte oppgaver kan utføres under ledelse av og delegering fra virksomhetens leder:

- vurdere evakuering og ekstraordinær tilintetgjøring av sikkerhetsgraderte dokumenter
- sikre systemer og utstyr i beskyttet område
- godkjenne besøk uten ledsagelse i beskyttet område
- beslutte om permanent adgang og om besøk til sperret område

Bestemmelser om virksomhetsledelsens utøvende ansvar for sikkerhetsoppgaver er gitt i ***forskrift om personellsikkerhet*** *og i* ***forskrift om informasjonssikkerhet.***

3 Sikkerhetsorganisering

Dette kapittelet gir veiledning i regelverkets bestemmelser om sikkerhetsorganisering, det vil si om organisering av arbeidet med å håndtere skjermingsverdig informasjon eller objekt.

Sikkerhetsorganisering omfatter delegering av utøvende ansvar og myndighet for arbeidsoppgaver med betydning for sikkerhet, tilrettelegging for riktig arbeidsutførelse, samt å sørge for at personellet bidrar til forebyggende sikkerhetstjeneste.

Virksomhetens sikkerhetsorganisering omfatter alle som utfører arbeidsoppgaver med betydning for sikkerhet. Virksomhetens sikkerhetsorganisasjon omfatter alle som utfører dedikerte sikkerhetsoppgaver, det vil si virksomhetsledelsen, foresatte og andre funksjoner med slike oppgaver.

3.1 Organisering for sikkerhet

Utøvende ansvar og myndighet knyttet til arbeidsoppgaver med betydning for sikkerhet må være avklart, formelt delegert og beskrevet.

Alle arbeidsoppgaver med betydning for sikkerhet må utføres planmessig og systematisk. Utøvende ansvar og myndighet må delegeres formelt og fremgå av stillingsbeskrivelse, arbeidsinstruks eller lignende. Dette gjelder for alle funksjoner i virksomheten som utfører arbeidsoppgaver med betydning for sikkerhet, og ikke kun for funksjonene i sikkerhetsorganisasjonen.

sikkerhetsloven § 5, 3. ledd *– om delegasjon av utøvende funksjoner*
forskrift om sikkerhetsadministrasjon § 3-5 *– om stillingsbeskrivelse el.*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Det må være klare skiller mellom utøvende og kontrollerende oppgaver.

Den forebyggende sikkerhetstjenesten må etableres slik at ikke enkeltpersoner, aktivt eller passivt, alene kan undergrave sikkerheten. Utøvende og kontrollerende oppgaver må derfor fordeles slik at ingen blir satt til å kontrollere eget arbeid.

Utøvende oppgaver kan eksempelvis være:

- journalføring av sikkerhetsgraderte dokumenter
- merking av maskinvare i informasjonssystem
- registrering av maskinlesbare lagringsmedier i medieregister
- vedlikehold av oversikt over nøkler for adgang til områder og oppbevaringsenheter

Kontrollerende oppgaver kan eksempelvis være:

- forberedelse av ledelsens evaluering av sikkerhetstilstanden i virksomheten
- planlegging og gjennomføring av interne sikkerhetsrevisjoner
- oppfølging og evaluering av korrigerende tiltak

Utøvende oppgaver utføres av en eller flere medarbeidere i det enkelte organisasjonsledd mens kontrollerende oppgaver må utføres i tilstrekkelig organisatorisk avstand fra utførelsen av de oppgavene som skal kontrolleres. Også kontrollerende oppgaver må følges opp. Eksempelvis er det aktuelt å kontrollere arbeidet med interne sikkerhetsrevisjoner, og da av andre enn dem som gjennomførte revisjonen.

merknad: I mindre virksomheter kan det være nødvendig å legge både kontrollerende og enkelte utøvende oppgaver til samme person. Slik oppgavefordeling må ikke medføre at personen

blir satt til å kontrollere eget arbeid. Det må fremgå av stillingsbeskrivelse, arbeidsinstruks eller lignende at vedkommende har flere funksjoner.

forskrift om sikkerhetsadministrasjon § 2-4 *– om fordeling av oppgaver*

Sikkerheten må ivaretas når personell fratrer, eller skifter stilling eller funksjon.

Autorisasjon for tilgang til sikkerhetsgradert informasjon må endres når tjenstlig behov endres. Personellets muligheter for tilgang og adgang, herunder rettigheter i informasjonssystem, må bringes i samsvar med gjeldende autorisasjon og eventuelt bringes til opphør.

Personellet må være kjent med at plikt til å bidra til forebyggende sikkerhetstjeneste, herunder taushetsplikt, består selv om arbeidsforholdet avsluttes.

Person som fratrer, eller skifter stilling eller funksjon, må:

- levere inn sikkerhetsgraderte dokumenter vedkommende har i sin besittelse
- levere inn nøkler, adgangskort eller lignende som gir tilgang til sikkerhetsgradert informasjon eller adgang til områder eller oppbevaringsenheter
- være informert om den taushetsplikt som gjelder etter avsluttet arbeidsforhold

sikkerhetsloven § 12, 1. ledd *– om taushetsplikt etter at arbeidet er avsluttet*
sikkerhetsloven § 24, 4. ledd, litra a og b *– om bortfall av autorisasjon*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Den forebyggende sikkerhetstjenesten må så langt det er praktisk og tjenlig samordnes med virksomhetens styringssystem for øvrig.

Forebyggende sikkerhetstjeneste må etableres planlagt og systematisk i form av et styringssystem for sikkerhet. Det er ofte nødvendig, og som regel hensiktsmessig, å samordne dette styringssystemet med virksomhetens øvrige styringsaktiviteter. Eksempelvis kan ivaretakelse og kontroll av sikkerhet integreres i øvrige aktiviteter ved å:

- gjennomføre ledelsens evaluering av den forebyggende sikkerhetstjenesten i eksisterende lederfora eller -møter
- se arbeidet med sikkerhetsrevisjoner i sammenheng med virksomhetens øvrige revisjonsaktiviteter
- samordne rapportering av uønskede hendelser overfor skjermingsverdig informasjon eller -objekt, med virksomhetens hendelsesrapportering for øvrig

forskrift om sikkerhetsadministrasjon § 1-1, 3. ledd *– om samordning av sikkerhetsadministrasjon*
forskrift om sikkerhetsadministrasjon § 2-2, 1. ledd *– om integrering i øvrige aktiviteter*

3.2 Sikkerhetsorganisasjonen

Sikkerhetsorganisasjonen må ha tilstrekkelig personell, kompetanse og verktøy.

Virksomhetens sikkerhetsorganisasjon omfatter funksjoner tillagt dedikerte sikkerhetsoppgaver, det vil si til virksomhetsledelsen, foresatte og alle andre med slike oppgaver.

Sikkerhetsorganisasjonen utpekes av virksomhetsledelsen. Slik utpeking alene er ikke tilstrekkelig for å oppnå en tilfredsstillende forebyggende sikkerhetstjeneste. Sikkerhetsorganisasjonen må også tildeles nødvendige ressurser i form av personell, kompetanse og utstyr. Videre må personellet gis nok tid til å utføre pålagte sikkerhetsoppgaver.

Sikkerhetsorganisasjonen må være i stand til å håndtere generelle sikkerhetsfaglige problemstillinger, og problemstillinger innen og på tvers av fagområdene som inngår i den forebyggende sikkerhetstjenesten. Sikkerhetsorganisasjonen må også være i stand til, eller kunne forsterkes til, å utføre nødvendige oppgaver i beredskapssituasjoner eller ved krise eller krig.

Dersom det er utpekt en beredskapsorganisasjon må forholdet mellom denne og sikkerhetsorganisasjonen for øvrig være avklart. Beredskapsorganisasjonens ansvar og myndighet, og vilkår for å tre i funksjon, må være fastlagt.

merknad: I mindre virksomheter kan det være nødvendig å samle flere utøvende sikkerhetsoppgaver hos en person, og det kan være nødvendig å gi utøvende ansvar for sikkerhetsoppgaver til personell som hovedsakelig har andre gjøremål. I slike situasjoner er det særlig viktig å påse at personellet har nok ressurser til å utføre sikkerhetsoppgavene og at ingen settes til å kontrollere eget arbeid.

forskrift om sikkerhetsadministrasjon § 2-1 *– om avsetting av nødvendige ressurser*
forskrift om sikkerhetsadministrasjon § 2-5, 1. og 2. ledd *– om utpeking av sikkerhetspersonell*
forskrift om sikkerhetsadministrasjon § 3-4 *– om forholdet mellom sikkerhetsorganisasjon og beredskapsorganisasjon*

Sikkerhetsleder må utpekes og inngå i sikkerhetsorganisasjonen.

Sikkerhetslederen forestår koordinering, rådgivning og kontroll ved utførelse av arbeidsoppgaver med betydning for sikkerhet. Mens ansvar for utøvelse er tillagt organisasjonen som helhet, med virksomhetsledelsen og foresatte som overordnet ansvarlige, er sikkerhetslederens funksjon i første rekke kontrollerende[3], eksempelvis:

- forberede ledelsens evaluering av sikkerhetstilstanden i virksomheten
- planlegge og gjennomføre interne sikkerhetsrevisjoner
- følge opp og evaluere korrigerende tiltak
- orientere virksomhetsledelsen om håndtering av uønskede hendelser
- forestå ekstern rapportering av uønskede hendelser, herunder rapportering av sikkerhetstruende hendelser til NSM

I tillegg er det naturlig at sikkerhetslederen utfører arbeidsoppgaver knyttet til veiledning, opplæring og i forbindelse med vedlikehold og distribusjon av styrende og utøvende sikkerhetsdokumenter. I virksomheter med et stort autorisasjonsbehov kan det også være aktuelt å gi sikkerhetslederen oppgaver knyttet til autorisering av personell.

Sikkerhetsleder må kunne rapportere direkte til virksomhetens leder. Utførelse av kontrollerende sikkerhetsoppgaver må skje i tilstrekkelig organisatorisk avstand fra utførelsen av de arbeidsoppgaver som skal kontrolleres. Det følger av dette at sikkerhetslederen må plasseres nær virksomhetsledelsen, og med tilstrekkelig avstand fra den delen av virksomheten vedkommende skal kontrollere.

Sikkerhetslederen må være norsk statsborger. NSM kan godkjenne at utenlandsk statsborger innehar denne funksjonen.

merknad: I mindre virksomheter kan det være nødvendig å legge enkelte utøvende sikkerhetsoppgaver til sikkerhetslederen. Oppgavefordelingen må ikke medføre at sikkerhetslederen blir satt til å kontrollere eget arbeid. De utøvende oppgavene må klart identifiseres i stillingsbeskrivelse, arbeidsinstruks eller lignende.

forskrift om sikkerhetsadministrasjon § 2-5 *– om sikkerhetsleder*
Ytterligere bestemmelser er gitt i ***forskrift personellsikkerhet.***

[3] Det vil si at sikkerhet "produseres i linjen" og kontrolleres av sikkerhetsleder.

Sikkerhetsorganisasjonen må omfatte de funksjoner som er nødvendig for å oppfylle sikkerhetsbehovet.

Sikkerhetsorganisasjonens omfang og utforming må stå i forhold til virksomhetens sikkerhetsbehov, omfang og kompleksitet. Når sikkerhetsbehovet tilsier det må sikkerhetsorganisasjonen utvides til å omfatte flere funksjoner.

Dersom virksomheten har kryptomateriell må det utnevnes kryptosikkerhetsleder og kryptoforvalter.

Ved større prosjekter, eller ved anskaffelser som involverer sikkerhetsgradert informasjon, må det utnevnes prosjektsikkerhetsleder. Prosjektsikkerhetslederens oppgaver i prosjektet tilsvarer de sikkerhetslederen har i virksomheten som helhet.

Dersom virksomheten benytter informasjonssystemer for behandling av sikkerhetsgradert informasjon, må det utnevnes datasikkerhetsleder. Datasikkerhetslederen forestår koordinering, rådgivning og kontroll av bruk, drift og vedlikehold av sikkerhetsgraderte informasjonssystemer.

Datasikkerhetslederens funksjon er i første rekke kontrollerende. Funksjonen må derfor plasseres med tilstrekkelig organisatorisk avstand fra utførelsen av de arbeidsoppgaver som skal kontrolleres. Datasikkerhetslederen kan gis mulighet til å rapportere direkte til virksomhetsledelsen, men bør av hensyn til behovet for enhetlig og samordnet sikkerhetsstyring rapportere til sikkerhetslederen.

Dersom virksomheten behandler personkontrollopplysninger må virksomhetens leder særskilt utpeke det personell som skal gis tilgang til slike opplysninger.

merknad: Dersom en avdeling, et tjenestested eller lignende har særlige sikkerhetsbehov kan det være aktuelt å samle sikkerhetsoppgaver hos en person, eksempelvis hos avdelingens sikkerhetsleder, avdelingens sikkerhetskontakt eller lignende. En slik organisering påvirker ikke den foresattes ansvar. Sikkerhetskontakten utfører utøvende sikkerhetsoppgaver på den foresattes vegne, og rapporterer til denne. Kontrollerende sikkerhetsoppgaver utføres på vegne av, og rapporteres til, sikkerhetsleder.

forskrift om sikkerhetsadministrasjon § 2-5, 1. ledd *– om sikkerhetsorganisasjonen og om kryptosikkerhetsleder og -forvalter*
forskrift om sikkerhetsadministrasjon § 2-6, 1. ledd *– om prosjektsikkerhetsleder*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet*** *og i* ***forskrift om personellsikkerhet.***

Stedfortredere for sentrale funksjoner i sikkerhetsorganisasjonen må utnevnes.

Det må utnevnes stedfortredere for sikkerhetsleder, kryptosikkerhetsleder og kryptoforvalter.

Også virksomhetsledelsen og foresatte må ha stedfortredere som ved fravær kan ivareta sikkerhetsledelse og utføre sikkerhetsoppgaver tillagt virksomhetsledelsen.

I den grad det er nødvendig for å sikre kontinuitet i den forebyggende sikkerhetstjenesten, må det også utnevnes stedfortreder for andre funksjoner i sikkerhetsorganisasjonen, eksempelvis for datasikkerhetsleder.

Stedfortrederens ansvar og myndighet, herunder hvilke sikkerhetsoppgaver (om ikke alle) som skal utføres når vedkommende fungerer, må være fastlagt. Også vilkår for å tre i funksjon, eksempelvis tidsgrense for fravær, må være fastlagt.

Stedfortredere må ha den kompetanse som er nødvendig for å utføre oppgavene i funksjonen de trer inn i og må gis nødvendig tid og ressurser til å utføre oppgavene.

merknad: I mindre virksomheter kan det være nødvendig at innehavere av funksjoner i sikkerhetsorganisasjonen er hverandres stedfortredere. Slik fungering er kun mulig når samme person samtidig kan utføre både egne og den andre funksjonens arbeidsoppgaver.

forskrift om sikkerhetsadministrasjon § 2-5, 1. ledd *– om sikkerhetsorganisasjonen og om stedfortredere*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

3.3 Kompetanse

Personellet må veiledes i og informeres om forebyggende sikkerhetstjeneste.

Personellet plikter å bidra til forebyggende sikkerhetstjeneste og må ha de holdninger og kunnskaper som er nødvendig for å oppfylle denne plikten, herunder må personellet ha kompetanse innen informasjonssystemsikkerhet når informasjonssystemer benyttes for behandling av sikkerhetsgradert informasjon.

De generelle sikkerhetstiltak og grunnleggende forholdsregler den enkelte er ment å ivareta må informeres om gjennom sikkerhetsinstruksen. Sikkerhetsbestemmelser knyttet til konkrete arbeidsoppgaver informeres om gjennom tiltaks- eller prosedyrebeskrivelsene. Informasjon må gis før personellet settes i tjeneste og deretter ved hver endring med betydning for sikkerhet.

Personellet må ved behov veiledes i forebyggende sikkerhetstjeneste slik at plikter er forstått og oppfylles og slik at arbeidsoppgaver med betydning for sikkerhet utføres som besluttet og med tilfredsstillende sikkerhet som resultat.

Den enkelte må kjenne til sin betydning for forebyggende sikkerhetstjeneste. Motivering og bevisstgjøring må gjennomføres jevnlig for å oppnå og bevare gode holdninger og for å skape forståelse for behovet for beskyttelse av skjermingsverdig informasjon og objekt.

sikkerhetsloven § 5, 2. ledd, litra a *– om sikkerhetsinstruks*
forskrift om sikkerhetsadministrasjon § 2-2 *– om foresattes veiledning av underordnede*
forskrift om sikkerhetsadministrasjon § 3-1 *– om veiledning av personell og om kjennskap til sikkerhetsbestemmelser*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Personellet må gis sikkerhetsfaglig opplæring.

Personellet må ha de kunnskaper og ferdigheter som er nødvendig for å utføre arbeidsoppgaver som besluttet. Personellet plikter å bidra til risikohåndtering og må opplæres i hvordan risiko overfor sikkerhetsgradert informasjon eller klassifisert objekt håndteres.

Opplæringen må omfatte grunnleggende opplæring i sikkerhet og opplæring tilpasset den enkeltes funksjon og arbeidsoppgaver. Opplæringen må i nødvendig grad gjennomføres som øving av arbeidsoppgaver. Dette gjelder særlig arbeidsoppgaver som sjeldent utføres, eksempelvis beredskapstiltak og -prosedyrer. Beredskapstiltak og -prosedyrer må øves jevnlig, minst årlig.

Kompetansebehov knyttet til arbeidsoppgaver og funksjoner må være avklart og fremgå av stillingsbeskrivelser, arbeidsinstrukser eller lignende. Opplæring må gjennomføres i henhold til plan som sikrer at nødvendig kompetanse oppnås og vedlikeholdes. Gjennomført opplæring registreres i kompetanseoversikt eller lignende.

sikkerhetsloven § 5, 2. ledd, litra b *– om opplæring i sikkerhetsspørsmål*
forskrift om sikkerhetsadministrasjon, § 3-2 *– om kompetanse og opplæring*
forskrift om sikkerhetsadministrasjon § 3-4, 2. ledd *– om beredskapsøvelser*
forskrift om sikkerhetsadministrasjon § 3-5 *– om beskrivelse av kompetansekrav*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

3.4 Den enkeltes plikter

Alt ansatt og innleid personell plikter å bidra til en effektiv forebyggende sikkerhetstjeneste.

Alle som utfører arbeidsoppgaver med betydning for sikkerhet plikter å overholde regelverkets bestemmelser og utføre pålagte arbeidsoppgaver som besluttet. Dette forutsetter kunnskap om regelverkets betydning for arbeidsutførelsen og om den forebyggende sikkerhetstjenesten.

Personellet plikter å bidra til håndtering av risiko overfor sikkerhetsgradert informasjon eller klassifisert objekt. Dette forutsetter forståelse for risiko og kompetanse nok til å håndtere risiko i en gitt situasjon.

Personellet plikter å bidra til kontinuerlig forbedring av den forebyggende sikkerhetstjenesten. Denne plikten oppfylles blant annet ved å melde fra om behov for endringer og muligheter for forbedringer og ved å rapportere uønskede hendelser.

Personellet har plikt til å opplyse om forhold som kan ha betydning for sikkerhetsklarering.

Personellet har taushetsplikt om sikkerhetsgradert informasjon og om utøvelsen av forebyggende sikkerhetstjeneste. Taushetsplikten består selv om arbeidsforholdet avsluttes.

sikkerhetsloven § 5, 4. ledd *– om plikt til å bidra i forebyggende sikkerhetstjeneste*
sikkerhetsloven § 12, 1. ledd *– om plikt til å beskytte sikkerhetsgradert informasjon (taushetsplikt)*
sikkerhetsloven § 24, 1. ledd *– medarbeiders plikt til å orientere autorisasjonsansvarlig*
forskrift om sikkerhetsadministrasjon § 2-3 *– om den enkeltes ansvar*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

3.5 Autorisasjon[4]

Personell må autoriseres før tilgang til sikkerhetsgradert informasjon gis.

Personell må autoriseres for tilgang til sikkerhetsgradert informasjon før slik tilgang gis[5]. Kun personell som har tjenstlig behov for tilgang til sikkerhetsgradert informasjon kan autoriseres. Personell som gjennom utførelse av arbeidsoppgaver kan få, men ikke trenger, tilgang til sikkerhetsgradert informasjon, autoriseres ikke. I stedet beskyttes informasjonen mot uautorisert tilgang.

Autorisasjonsansvarlig må fastsette nødvendig klarerings- og autorisasjonsnivå, anmode om personkontroll og autorisere personell for tilgang til sikkerhetsgradert informasjon. Autorisasjonen må endres når det tjenstlige behovet endres.

Dersom det fremkommer opplysninger som gir grunn til tvil om en autorisert person kan anses sikkerhetsmessig skikket må autorisasjonsansvarlig vurdere autorisasjonen tilbakekalt, nedsatt eller suspendert.

Informasjon om autorisasjoner må være tilgjengelig for de som distribuerer sikkerhetsgradert informasjon i virksomheten, eksempelvis ved at autorisasjonsoversikt, -liste eller lignende gjøres tilgjengelig for arkivpersonell.

merknad: I virksomheter med et stort autorisasjonsbehov kan myndigheten til å gi autorisasjon delegeres. Alternativt kan virksomhetslederen autorisere etter autorisasjonssamtaler utført av andre, eksempelvis foresatt eller sikkerhetsleder.

sikkerhetsloven § 19, 1. ledd *– om autorisasjon for tilgang til skjermingsverdig informasjon*
sikkerhetsloven § 20, 1. og 6. ledd *– om anmodning om personkontroll*
sikkerhetsloven § 23, 5. ledd *– om autorisasjon*
sikkerhetsloven § 24, 1., 3. og 5. ledd *– om orientering og varsling av autorisasjonsansvarlig, og vurdering av autorisasjon*
forskrift om sikkerhetsadministrasjon § 2-2, 2. ledd *– om informasjon til autorisasjonsansvarlig*
Ytterligere bestemmelser om autorisasjon er gitt i ***forskrift om personellsikkerhet*** *og i* ***forskrift om informasjonssikkerhet.***

[4] Ytterligere veiledning om autorisasjon er gitt i Nasjonal sikkerhetsmyndighets ”Veiledning til sikkerhetslovens kapittel 6 og forskrift om personellsikkerhet”, samt i NSMs ”Autorisasjonshåndbok”.

[5] Personell må sikkerhetsklareres før de autoriseres for tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere.

4 Sikkerhetstiltak og -prosedyrer

Dette kapittelet gir veiledning i regelverkets bestemmelser om sikkerhetstiltak og -prosedyrer begrenset til korte beskrivelser av regelverkets mest sentrale bestemmelser om slike tiltak og prosedyrer.

Regelverkets bestemmelser om sikkerhetstiltak og -prosedyrer er minimumskrav. Virksomheten må selv avdekke behov for ytterligere tiltak og prosedyrer med utgangspunkt i risikovurderinger[6]. Avhengig av risiko og hvordan sikkerhetsgradert informasjon og klassifiserte objekter håndteres i virksomheten er det aktuelt å etablere sikkerhetstiltak og prosedyrer innen fagområdene[7]:

- personellsikkerhet
- dokumentsikkerhet
- informasjonssystemsikkerhet
- fysisk sikring
- kryptosikkerhet
- kurerposttjeneste
- tempestsikkerhet
- sikkerhetsgraderte anskaffelser

Sikkerhetstiltak og -prosedyrer kan virke forebyggende og reaktivt, kan veilede og tvinge adferd – og kan forhindre, gjøre det mulig å oppdage og kompensere sikkerhetsbrudd. Alle disse formene for sikkerhetstiltak og -prosedyrer er aktuelle, enkeltvis og i kombinasjon.

Det må avsettes nødvendige ressurser for etablering av sikkerhetstiltak og -rutiner, herunder må det avsettes tilstrekkelig tid for utvikling og utprøving av slike tiltak og rutiner.

4.1 Sikkerhetsgradering og klassifisering

Skjermingsverdig informasjon må sikkerhetsgraderes i forhold til den skade som kan oppstå dersom informasjonen blir kjent for uvedkommende.

Sikkerhetsgradering er resultatet av vurdering av skade som kan oppstå dersom skjermingsverdig informasjon blir kjent for uvedkommende. Dokumenter og maskinlesbare lagringsmedier merkes med sikkerhetsgradering for å varsle personellet som håndterer informasjonen om sikkerhetsbehov og om hvilke sikkerhetstiltak og -prosedyrer som gjelder.

Skjermingsverdig informasjon sikkerhetsgraderes av den som tilvirker informasjonen. Det er som hovedregel kun tilvirker som kan beslutte avgradering eller nedgradering, uavhengig av hvor informasjonen befinner seg. Ved omgradering skal tilvirker informere alle som har mottatt informasjonen.

Som norsk sikkerhetsgradering benyttes BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG. Fremmed stat eller internasjonal organisasjon benytter andre sikkerhetsgraderinger for den informasjon de utsteder. Slik informasjon håndteres etter egne regler med utgangspunkt i bestemmelsene for håndtering av norsk sikkerhetsgradert informasjon.

sikkerhetsloven § 11 *– om sikkerhetsgradering av informasjon*

Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

[6] Veiledning knyttet til regelverkets bestemmelser om risikohåndtering og risikovurdering er gitt i kapittel 8.

[7] Mer detaljert informasjon knyttet til bestemmelser om sikkerhetstiltak og -prosedyrer innen forskjellige fagområder er tilgjengelig fra NSM, blant annet i egne veiledninger.

Skjermingsverdig objekt må klassifiseres i forhold til den skade som kan oppstå dersom objektet utsettes for sikkerhetstruende virksomhet.

Klassifisering er resultatet av vurderingen av skade som kan oppstå dersom skjermingsverdig objekt får redusert funksjonalitet, blir utsatt for skadeverk eller ødeleggelse eller blir overtatt av uvedkommende.

Hvert enkelt departement utpeker skjermingsverdige objekter innen sitt myndighetsområde. Objekteier foreslår overfor departementet hvilke objekter som er skjermingsverdige.

Som klassifisering benyttes VIKTIG, KRITISK eller MEGET KRITISK.

sikkerhetsloven §§ 17 og 17b *– om klassifisering av skjermingsverdig objekt*

4.2 Sikkerhetsklarering[8]

Personell må sikkerhetsklareres før det gis tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere.

Personell med tjenstlig behov for tilgang til informasjon sikkerhetsgradert KONFIDENSIELT eller høyere må sikkerhetsklareres før de autoriseres for slik tilgang. Personell som gjennom utførelse av arbeidsoppgaver kan få, men ikke trenger, tilgang til sikkerhetsgradert informasjon sikkerhetsklareres kun når det ikke er mulig å etablere tilfredsstillende tiltak mot uautorisert tilgang.

Sikkerhetsklarering gis når personkontroll ikke avdekker rimelig tvil om personens sikkerhetsmessige skikkethet. Personkontrollen innebærer vurdering av pålitelighet, lojalitet og sunn dømmekraft i forhold til behandling av skjermingsverdig informasjon.

Sikkerhetsklarering gis for graderingsnivåene:

- KONFIDENSIELT (ev. NATO CONFIDENTIAL eller tilsvarende)
- HEMMELIG (ev. NATO SECRET eller tilsvarende)
- STRENGT HEMMELIG (ev. COSMIC TOP SECRET eller tilsvarende)

Personkontroll iverksettes etter anmodning fra autorisasjonsansvarlig til klareringsmyndigheten.

Hvert enkelt departement er klareringsmyndighet for personell innen sitt myndighetsområde og for personell ansatt hos leverandør i sikkerhetsgradert anskaffelse. Departementet kan delegere klareringsmyndighet til underlagte virksomheter og til anskaffelsesmyndigheter.

Fylkesmannen[9] er klareringsmyndighet for personell i fylkeskommune, kommune og virksomheter med beredskapsmessig tilknytning til disse. Fylkesmannen er også klareringsmyndighet for personell ansatt hos leverandør i sikkerhetsgradert anskaffelse foretatt av en fylkeskommunal eller kommunal virksomhet.

For tilgang til informasjon sikkerhetsgradert BEGRENSET er det ikke nødvendig med sikkerhetsklarering, men personellet må være autorisert.

sikkerhetsloven §§ 19 – 26 *– om sikkerhetsklarering*
Ytterligere bestemmelser er gitt i ***forskrift om personellsikkerhet.***

[8] Ytterligere veiledning om sikkerhetsklarering er gitt i Nasjonal sikkerhetsmyndighets "Veiledning til sikkerhetslovens kapittel 6 og forskrift om personellsikkerhet".

[9] Fylkesmennenes klareringsmyndighet er tillagt fylkesmannen i Oslo og Akershus og fylkesmannen i Rogaland.

4.3 Tiltak og prosedyrer for et sammensatt sikkerhetsbehov

Det må iverksettes sikkerhetstiltak og -prosedyrer for å oppfylle sammensatte sikkerhetsbehov.

Klassifisert objekt må beskyttes slik at objektets funksjonalitet opprettholdes, det vil si sikring av tilgjengelighet for viktige og kritiske funksjoner,

Sikkerhetsgradert informasjon må beskyttes for å hindre kompromittering, det vil si sikring av informasjonens konfidensialitet, tilgjengelighet og integritet.

Ved bruk av informasjonssystemer for behandling av sikkerhetsgradert informasjon må også iverksettes tiltak for å sikre:

- informasjonens autentisitet
- at brukere kan holdes ansvarlig for handlinger i informasjonssystemet
- tillit til at sikkerhetstiltak er korrekt implementert og ivaretar sikkerhet på en effektiv og hensiktsmessig måte

sikkerhetsloven § 12, 2. ledd *– om nærmere regler for å sikre korrekthet, fullstendighet og tilgjengelighet*
forskrift om sikkerhetsadministrasjon § 1-2, 1. ledd *– kompromittering definert*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

4.4 Beredskap

Det må være beredskap for situasjoner som innebærer økt risiko overfor sikkerhetsgradert informasjon eller klassifisert objekt.

Sikkerhetstiltak og -prosedyrer for beredskapssituasjoner, krise eller krig må være forberedt.

Beredskapstiltak og -prosedyrer må gi nødvendig forsterkning av den forebyggende sikkerhetstjenesten. De må omfatte særskilte tiltak og prosedyrer som skal iverksettes etter behov, eksempelvis tiltak og prosedyrer for evakuering og nødmakulering av sikkerhetsgradert informasjon.

Dersom det er utpekt en beredskapsorganisasjon må ansvar og myndighet og vilkår for å tre i funksjon være fastlagt.

Beredskapstiltak og -prosedyrer må prøves ut og kontinuerlig forbedres gjennom årlig øving.

forskrift om sikkerhetsadministrasjon § 3-4, 2. ledd *– om beredskapstiltak og beredskapsorganisasjon*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

4.5 Sikkerhetsgodkjenning

Informasjonssystemer må være sikkerhetsgodkjente før de tas i bruk for behandling av sikkerhetsgradert informasjon.

Informasjonssystemer må sikkerhetsgodkjennes i forhold til bruksmåte og graderingsnivå før de tas i bruk for behandling av sikkerhetsgradert informasjon. Ved sikkerhetsgodkjenning vurderes både sikkerhetstiltak og -prosedyrer som er etablert i selve informasjonssystemet og systemspesifikke sikkerhetstiltak og -prosedyrer som forutsettes iverksatt der informasjonssystemet skal tas i bruk.

Sikkerhetsgodkjenning gis av Nasjonal sikkerhetsmyndighet eller etter delegering fra Nasjonal sikkerhetsmyndighet. For enkelte kombinasjoner av bruksmåte og graderingsnivå er virksomheten selv godkjenningsmyndighet.

Sikkerhetsgodkjent informasjonssystem og tilknyttet utstyr må merkes med den høyeste sikkerhetsgradering det kan benyttes for. Merkingen er et varsel til personellet som benytter utstyret

om hvilken informasjon som kan behandles og om hvilke sikkerhetstiltak og -prosedyrer som gjelder. Transportable informasjonssystemer må merkes diskret slik at merkingen ikke gjør systemet attraktivt for uvedkommende.

Informasjon om sikkerhetsgodkjente informasjonssystemer og tilknyttet utstyr skal fremgå av godkjenningsdokumentasjon og av konfigurasjonsoversikter, systemoversikter eller lignende.

sikkerhetsloven § 13, 1. ledd *– om godkjenning av informasjonssystem*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Kryptosystemer og kryptoinstallasjoner må være godkjente før de tas i bruk for beskyttelse av sikkerhetsgradert informasjon.

Ved kommunikasjon av sikkerhetsgradert informasjon utenfor eget kontrollert område må det benyttes kryptering. Kryptosystemer, -utstyr og -installasjoner godkjennes av NSM. Også mottak og bruk av kryptomateriell må godkjennes.

Oversikt over kryptomateriellet, herunder oversikt over kryptosystemer og -utstyr, må fremgå av kryptoregnskap.

sikkerhetsloven § 14, 1. ledd *– om godkjenning av kryptoutstyr, leverandør av kryptomateriell og kryptoalgoritme*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

5 Forholdet til andre virksomheter

Dette kapittelet gir veiledning i regelverkets bestemmelser om forholdet til virksomheter som kan ha betydning for sikkerhet, det vil si om hvordan forebyggende sikkerhetstjeneste utøves virksomheter i mellom.

Handlinger hos andre virksomheter kan ha innvirkning på den forebyggende sikkerhetstjenesten i virksomheten og virksomhetens handlinger kan ha betydning for sikkerheten hos andre. Behov og plikter kan derfor ikke utelukkende oppfylles innen virksomhetens grenser.

Forebyggende sikkerhetstjeneste over organisasjonsgrense forutsetter forståelse for hverandres sikkerhetsbehov, kjennskap til hverandres sikkerhetstjeneste, klare ansvars- og myndighetsforhold og samarbeid.

5.1 Formidling av sikkerhetsgradert informasjon til andre

Sikkerhetsgradert informasjon kan kun formidles til virksomheter som lovlig kan behandle slik informasjon.

Sikkerhetsgradert informasjon kan kun formidles til virksomheter som har tjenstlig behov for å behandle slik informasjon.

Sikkerhetsgradert informasjon kan kun formidles til virksomheter sikkerhetsloven gjelder for og som er autorisert for behandling av slik informasjon. Det kan ikke formidles informasjon med høyere sikkerhetsgradering enn det mottakeren er autorisert for.

Avhengig av graderingsnivå, og hvor mottakeren befinner seg, sendes informasjonen i vanlig postsending, som registrert postsending eller med kurer. Ved elektronisk kommunikasjon av sikkerhetsgradert informasjon utenfor eget kontrollert område må det benyttes kryptering.

Det er utsteder som sikkerhetsgraderer skjermingsverdig informasjon, og kun utsteder som kan omgradere slik informasjon. Mottaker av informasjonen påtar seg å beskytte informasjonen i samsvar med graderingsnivået, men har samtidig ansvar for å melde fra om informasjon som ikke har riktig sikkerhetsgradering.

sikkerhetsloven § 2 *– om hvem sikkerhetsloven gjelder for*
sikkerhetsloven § 11 *– om sikkerhetsgradering*
sikkerhetsloven § 12 *– om plikt til å beskytte sikkerhetsgradert informasjon*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

5.2 Leveranser med betydning for sikkerheten

Virksomheten må være i stand til å fastsette og følge opp krav til forebyggende sikkerhetstjeneste når andre utfører arbeidsoppgaver for virksomheten.

Den forebyggende sikkerhetstjenesten må omfatte arbeidsoppgaver med betydning for sikkerheten som innleid personell eller leverandører utfører på virksomhetens vegne. Virksomheten må derfor ha tilstrekkelig bestillerkompetanse til å fastsette og følge opp krav til forebyggende sikkerhetstjeneste når slike oppgaver overlates til andre.

Sikkerhetsbestemmelser og ansvars- og myndighetsfordeling må fremgå av avtale.

sikkerhetsloven § 5 *– om plikt til å utøve forebyggende sikkerhetstjeneste*
forskrift om sikkerhetsadministrasjon § 2-1, 1. ledd *– om virksomhetsledelsens ansvar*
forskrift om sikkerhetsadministrasjon § 2-2, 1. ledd *– om foresattes ansvar overfor private leverandører*

Innleid personell har plikt til å bidra til forebyggende sikkerhetstjeneste og må gis mulighet til å oppfylle denne plikten.

Innleid personell som utfører arbeidsoppgaver med betydning for sikkerheten må behandles tilsvarende virksomhetens egne medarbeidere. Dette innebærer at innleid personell må:

- sikkerhetsklareres og autoriseres i samsvar med tjenstlig behov, for tilgang til sikkerhetsgradert informasjon
- informeres om og veiledes i hvordan den forebyggende sikkerhetstjenesten utføres i virksomheten
- gis nødvendig opplæring for å oppnå og opprettholde den kompetanse som er nødvendig
- pålegges den samme plikt som virksomhetens medarbeidere har til å bidra til forebyggende sikkerhetstjeneste, herunder taushetsplikt

Avtale med innleid personell må i nødvendig omfang omfatte sikkerhetsbestemmelser, herunder bestemmelser om taushetsplikt.

Virksomheten må ha oversikt over hvilket personell hos andre virksomheter som har nødvendig sikkerhetsklarering, autorisasjon og kompetanse til å utføre arbeidsoppgaver for virksomheten.

sikkerhetsloven § 5, 2. ledd, litra b *– om opplæring av engasjert personell i sikkerhetsspørsmål*
sikkerhetsloven § 5, 4. ledd *– om innleid personells plikter*
sikkerhetsloven § 12, 1. ledd *– om taushetsplikt*
sikkerhetsloven § 24, 1, ledd *– om personellets plikt til å orientere autorisasjonsansvarlig*
forskrift om sikkerhetsadministrasjon § 2-2, 1. ledd *– om foresattes ansvar overfor private leverandører*
forskrift om sikkerhetsadministrasjon § 2-3 *– om innelid personells plikter*
forskrift om sikkerhetsadministrasjon § 3-1 *– om veiledning av personell og om kjennskap til sikkerhetsbestemmelser*
forskrift om sikkerhetsadministrasjon, § 3-2 *– om kompetanse og opplæring*
Ytterligere bestemmelser er gitt i ***forskrift om personellsikkerhet*** *og i* ***forskrift om informasjonssikkerhet.***

Leveranser som forutsetter at leverandøren gis tilgang til sikkerhetsgradert informasjon må utføres av virksomheter som lovlig kan behandle slik informasjon.

Leveranser som forutsetter at leverandøren, og ikke kun innleid personell, gis tilgang til sikkerhetsgradert informasjon kan kun utføres av virksomheter sikkerhetsloven gjelder for. Dette innebærer at leveransen må utføres av annet forvaltningsorgan eller som en sikkerhetsgradert anskaffelse.

Dersom leveransen utføres av annet forvaltningsorgan påtar dette organet seg å beskytte den sikkerhetsgraderte informasjonen i samsvar med graderingsnivået gjennom utøvelse av egen forebyggende sikkerhetstjeneste.

Dersom leveransen utføres som sikkerhetsgradert anskaffelse må det inngås sikkerhetsavtale mellom leverandør og anskaffelsesmyndighet og leverandøren må ha leverandørklarering. Den som anskaffer varer eller tjenester fra andre enn forvaltningsorganer er anskaffelsesmyndighet.

Den som anskaffer varer eller tjenester er overordnet ansvarlig for sikkerheten hos leverandøren. Leverandøren påtar seg ansvaret for sikkerheten i egen virksomhet og utøver dette ansvaret gjennom å etablere en forebyggende sikkerhetstjeneste.

Anskaffelsesmyndigheten må ha oversikt over sikkerhetsgraderte anskaffelser og over de leverandører som benyttes. NSM må oversendes kopi av de sikkerhetsavtaler som inngås og må fortløpende meddeles eventuelle endringer i slike avtaler.

sikkerhetsloven § 2 *– om hvem sikkerhetsloven gjelder for*
sikkerhetsloven § 3, 1. ledd, nr 13 *– anskaffelsesmyndighet definert*
sikkerhetsloven § 27 *– om sikkerhetsavtale*

sikkerhetsloven § 28 *– om leverandørklarering*
forskrift om sikkerhetsadministrasjon § 2-6 *– om ansvar for sikkerhet ifm. anskaffelser*
Ytterligere bestemmelser er gitt i ***forskrift om sikkerhetsgraderte anskaffelser.***

5.3 Overordnet og underordnet virksomhet

Overordnet virksomhet er ansvarlig for sikkerheten i underordnede virksomheter.

Virksomheten kan autorisere underlagte virksomheter for behandling av sikkerhetsgradert informasjon forutsatt at det er tjenstlig behov for slik behandling. Autorisasjonen kan kun gis innenfor rammen av den autorisasjon virksomheten selv har, herunder kun til og med det graderingsnivå virksomheten selv er autorisert for.

Virksomhetsledelsen er ansvarlig for utøvelsen av forebyggende sikkerhetstjeneste i underlagte virksomheter. Dette ansvaret kan utøves ved å:

- sørge for at det avsettes nødvendige ressurser for å ivareta forebyggende sikkerhetstjeneste i underlagte virksomheter
- bidra til etableringen av forebyggende sikkerhetstjeneste
- følge opp at sikkerhetstjenesten er etablert som besluttet og gir tilfredsstillende sikkerhet som resultat

Føringer og bestemmelser for den forebyggende sikkerhetstjenesten i underordnede virksomheter kan eksempelvis gis gjennom instrukser, iverksettelsesbrev eller lignende.

forskrift om sikkerhetsadministrasjon § 2-1, 1. ledd *– om ansvar for sikkerhetstjenesten i underlagte virksomheter*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Sikkerhet må ivaretas når to eller flere virksomheter er tilkoblet samme informasjonssystem.

Dersom to eller flere virksomheter er tilkoblet et felles informasjonssystem påhviler ansvaret for sikkerhet i informasjonssystemet felles overordnet virksomhet. Alternativt kan den overordnede virksomheten utpeke en ansvarlig for sikkerhet, eller de tilkoblede virksomhetene kan avtale seg i mellom hvem som skal være ansvarlig.

Slik avtale må angi hvilket graderingsnivå informasjonssystemene er sikkerhetsgodkjent for og hvilke sammenkoblinger med andre informasjonssystemer som tillates.

forskrift om sikkerhetsadministrasjon § 2-6, 3. ledd *– om ansvar for felles informasjonssystem*

Departementer utpeker skjermingsverdige objekter innen sitt myndighetsområde.

Det enkelte departement er ansvarlig for utpeking av skjermingsverdige objekter innen sitt myndighetsområde.

Objekteier foreslår overfor departementet hvilke objekter som er skjermingsverdige og plikter å beskytte klassifisert objekter med sikkerhetstiltak.

sikkerhetsloven §§ 17 og 17b *– om utpeking og beskyttelse av skjermingsverdig objekt*

6 Sikkerhetsoppfølging

Dette kapittelet gir veiledning i regelverkets bestemmelser om oppfølging av den forebyggende sikkerhetstjenesten, det vil si om etterprøving av sikkerhetstjenesten og beslutninger om nødvendige endringer.

Sikkerhetsoppfølging gjennomføres som undersøkelser og evaluering av den forebyggende sikkerhetstjenesten, rapportering av uønskede hendelser, og gjennom beslutninger om og iverksetting av korrigerende tiltak.

Endringer i interne og eksterne forhold påvirker sikkerhetsbehovet og kan gjøre det nødvendig med tilpassing og forbedring av den forebyggende sikkerhetstjenesten. Slik kontinuerlig sikkerhetsforbedring forutsetter oppdatert kunnskap om sikkerhetstjenestens utøvelse og funksjon.

6.1 Ledelsens evaluering

Virksomhetsledelsen må minst en gang i året evaluere sikkerhetstilstanden i virksomheten.

Målet for ledelsens evaluering er å avklare hvorvidt den forebyggende sikkerhetstjenesten er tilstrekkelig, det vil si om sikkerhetsgradert informasjon eller klassifisert objekt er tilfredsstillende beskyttet. Evalueringen gjennomføres som et møte som, resulterer i nødvendige beslutninger om tilpassing og forbedring av sikkerhetstjenesten.

Sikkerhetstjenesten må forbedres når sikkerhetsrevisjoner eller hendelseshåndtering avdekker systematiske avvik. Også endringer i interne eller eksterne forutsetninger, eksempelvis nye trusler, endringer i organisasjon, lokaler, informasjonsbehandling eller i regelverket, kan gjøre det nødvendig med forbedringer.

God evaluering av sikkerhetstilstanden forutsetter kjennskap til trusler og trusselaktører basert på informasjon fra interne og eksterne kilder[10]. Også kunnskap om sårbarheter og om sikkerhetstjenestens utøvelse og funksjon må inngå i evalueringen. Slik kunnskap baseres på informasjon om resultater fra sikkerhetsrevisjoner og fra håndteringen av uønskede hendelser.

Resultater fra ledelsens evalueringer må dokumenteres i form av referat som angir ev. beslutninger om tilpassinger og forbederinger av den forebyggende sikkerhetstjenesten.

sikkerhetsloven § 5, 2.ledd, litra c *– om regelmessig kontroll av sikkerhetstilstanden*
forskrift om sikkerhetsadministrasjon § 4-4, 2. ledd *– om ledelsens evaluering*
forskrift om sikkerhetsadministrasjon § 4-4, 3. ledd *– om dokumentering av resultater fra evalueringer*

6.2 Sikkerhetsrevisjon

Virksomheten må planlegge og gjennomføre interne sikkerhetsrevisjoner.

Målet for interne sikkerhetsrevisjoner er å avklare hvorvidt den forebyggende sikkerhetstjenesten gjennomføres som besluttet, fungerer som forutsatt og er i samsvar med regelverket. Dersom det i sikkerhetsrevisjoner avdekkes avvik, enten fra interne bestemmelser eller fra regelverket, må det iverksettes korrigerende tiltak for å begrense skade og hindre gjentagelse.

Sikkerhetsrevisjoner må gjennomføres regelmessig, det vil si i henhold til plan. Revisjonene bør planlegges slik at hele den forebyggende sikkerhetstjenesten undersøkes mellom ledelsens evaluering av sikkerhetstilstanden. Det vil si at hele sikkerhetstjenesten bør undersøkes i løpet av 12 måneder.

[10] Eksempelvis Nasjonal sikkerhetsmyndighets Sikkerhetsvarsler og Rapport om sikkerhetstilstanden.

Dersom virksomheten velger å forskyve eller forsinke enkelte undersøkelser, må dette begrunnes – eksempelvis med at det i deler av virksomheten har vært liten aktivitet, ingen uønskede hendelser, eller at sikkerhetstjenestens utøvelse og funksjon er avklart på annen måte.

Sikkerhetsrevisjoner kan omfatte gjennomganger av sikkerhetsdokumentasjon, intervjuer med personellet, og prøving av tekniske sikkerhetstiltak[11]. Sikkerhetsrevisjoner må når det er aktuelt omfatte:

- kontroll med tilstedeværelse av sikkerhetsgraderte dokumenter og maskinlesbare lagringsmedier
- opptelling av nøkler for tilgang til områder og oppbevaringsenheter
- kontroll med beholdning av kryptomateriell

Sikkerhetsrevisjoner må gjennomføres etter god faglig standard for slike undersøkelser, herunder må det være tilstrekkelig organisatorisk avstand mellom den som utfører revisjonen og utførelsen av de arbeidsoppgaver som skal kontrolleres.

Resultater fra sikkerhetsrevisjoner må dokumenteres i form av revisjonsrapporter Rapportene fremlegges for virksomhetsledelsen.

merknad: I større virksomheter kan det være nødvendig å utforme revisjonsprogrammet slik at sikkerhetsrevisjoner (”delrevisjoner”) fordeles over året. Mindre virksomheter kan gjennomgå hele sikkerhetstjenesten i en revisjon, eventuelt som del av foreberedelsen til ledelsens evaluering av sikkerhetstilstanden.

sikkerhetsloven § 5, 2.ledd, litra c *– om regelmessig kontroll av sikkerhetstilstanden*
forskrift om sikkerhetsadministrasjon § 4-4, 1. og 3. ledd *– om sikkerhetsrevisjon og dokumentering av resultater*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

6.3 Håndtering av uønskede hendelser

Uønskede hendelser må rapporteres og registreres internt i virksomheten.

Feil og mangler ved den forebyggende sikkerhetstjenesten og sikkerhetstruende hendelser er uønskede hendelser i den forebyggende sikkerhetstjenesten.

Feil og mangler må rapporteres til foresatt og kan eksempelvis være:

- mulig forbedring av den forebyggende sikkerhetstjenesten
- forhold som ikke er sikkerhetsbrudd, men som det er nødvendig å følge opp, eksempelvis avvik fra interne bestemmelser
- sikkerhetsbrudd (som ikke er ”grove”)

Sikkerhetstruende hendelser må omgående rapporteres til foresatt som meddeler virksomhetsledelsen og kan eksempelvis være:

- sikkerhetstruende virksomhet, dvs. forberedelse til, (forsøk på) gjennomføring av og medvirkning til spionasje, sabotasje eller terrorhandlinger
- kompromittering, det vil si tap, eller mistanke om tap, av konfidensialitet, tilgjengelighet eller integritet for sikkerhetsgradert informasjon
- grove sikkerhetsbrudd, det vil si sikkerhetsbrudd som direkte kan medføre sikkerhetstruende virksomhet eller kompromittering, samt sikkerhetsbrudd som skyldes systematiske avvik

[11] NSM kan anmodes om gjennomføring av tekniske sikkerhetsundersøkelser og inntregningstesting, eksempelvis som bistand til virksomhetens arbeid med interne sikkerhetsrevisjoner

Også:

- mistanke om kompromittering av sikkerhetsgradert informasjon fremkommet under tekniske undersøkelser
- feil eller mangelfull rapportering av krytptoregnskap
- sikkerhetsbrudd ved nødrett og nødverge

… skal rapporteres som sikkerhetstruende hendelser.

Det må etableres system i form av prosedyrer og verktøy for rapportering av uønskede hendelser. Rapporteringssystemet må være kjent for personellet.

Informasjon om sikkerhetstruende hendelser, og om korrigeringen av dem, må registreres. Også feil og mangler ved den forebyggende sikkerhetstjenesten bør registreres. Informasjon om kompromittering av informasjon sikkerhetsgradet KONFIDENSIELT eller høyere må også registreres i den journal eller lignende hvor den kompromitterte informasjonen er registrert.

sikkerhetsloven § 3, nr. 2 *– sikkerhetstruende virksomhet definert*
forskrift om sikkerhetsadministrasjon § 1-2, nr. 2 – 4 *– om sikkerhetstruende hendelse, kompromittering og sikkerhetsbrudd*
forskrift om sikkerhetsadministrasjon § 2-2 *– om rapportering av manglende skikkethet*
forskrift om sikkerhetsadministrasjon § 2-3, 2. ledd, nr. 5 og 6 *– om personellets rapportering*
forskrift om sikkerhetsadministrasjon § 5-3 *– om nødrett og nødverge*
forskrift om sikkerhetsadministrasjon § 5-4 *– om rapportering og registrering av sikkerhetstruende hendelser*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Sikkerhetstruende hendelser må rapporteres til NSM.

Alle sikkerhetstruende hendelser må rapporteres til NSM, herunder mistanke om ulovlig avlytting av, eller innsyn i, rom som er permanent sikret mot teknisk avlytting eller innsyn, samt brudd på bestemmelser for slike rom.

Også sikkerhetsbrudd (som ikke er ”grove”) som berører informasjon sikkerhetsgradert av utenlandsk myndighet eller internasjonal organisasjon, må rapporteres til NSM.

Rapporteringen må omfatte:

- foreløpig rapport som sendes snarest mulig etter at hendelsen eller bruddet oppdages
- utfyllende rapporter når ny, viktig informasjon fremkommer
- endelig rapport når saken anses avsluttet, med sammenfatning av alle opplysninger og undersøkelser og med informasjon om gjennomførte og planlagte tiltak

Rapporter kan slås sammen når saken avsluttes kort tid etter at hendelsen eller bruddet ble oppdaget.

Rapporten må når det er aktuelt omfatte kopi av tilvirkers skadevurdering etter kompromittering av informasjon sikkerhetsgradert KONFIDENSIELT eller høyere.

forskrift om sikkerhetsadministrasjon § 5-2 *– om oversendelse av kopi av skaderapport*
forskrift om sikkerhetsadministrasjon § 5-6 *– om rapportering av sikkerhetstruende hendelser*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Sikkerhetstruende hendelser må vurderes rapportert til politiet.

Ved sikkerhetstruende hendelse må det vurderes å orientere politiet eller om forholdet skal anmeldes. NSM må underrettes om politianmeldelser.

forskrift om sikkerhetsadministrasjon § 5-7 *– om orientering og anmeldelse til politiet ved sikkerhetstruende hendelser*

Uønskede hendelser må korrigeres, for å begrense skade og hindre gjentagelse

Korrigering av uønskede hendelser gjennomføres ved tiltak som begrenser og motvirker skade og ved tiltak som hindrer gjentagelse gjennom korrigering av underliggende årsaker.

Feil og mangler kan korrigeres gjennom forbedring, tilpassing eller presisering av sikkerhetstiltak og -prosedyrer.

Sikkerhetstruende hendelser korrigeres ved å:

- undersøke omstendighetene ved hendelsen, sikre ev. bevis og gjennomgå relevante rutiner og systemer
- iverksette umiddelbare tiltak for å redusere skadeomfanget
- om nødvendig iverksette midlertidige eller permanente sikkerhetstiltak for å hindre gjentagelse
- vurdere reaksjon overfor ansvarlige personer

Korrigerende tiltak ved kompromittering av informasjon gradert KONFIDENSIELT eller høyere må blant annet ta utgangspunkt i utsteders skadevurdering med redegjørelse for aktuelle tiltak som kan redusere skaden.

forskrift om sikkerhetsadministrasjon § 4-3 *– korrigering av sikkerhetstiltak*
forskrift om sikkerhetsadministrasjon § 4-4, 1. ledd *– om avklaring av tiltak som skal iverksettes*
forskrift om sikkerhetsadministrasjon § 5-1 *– om håndtering av sikkerhetsturende hendelser*
forskrift om sikkerhetsadministrasjon § 5-2 *– om skadevurdering ved kompromittering av informasjon*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

6.4 Sikkerhetsoppfølging av andre virksomheter

Ledelsens evaluering må omfatte vurdering sikkerhetstilstanden hos andre virksomheter, herunder hos underlagte virksomheter.

Ledelsens evaluering må omfatte bruk av innleide og av leverandører, samt vurdering av behov for endringer i slik bruk. Evalueringen må resultere i nødvendige beslutninger om inngåelse, endring eller avslutting av avtaleforhold.

Sikkerhetstilstanden hos underlagte virksomheter kan vurderes med utgangspunkt i informasjon om resultater fra sikkerhetsrevisjoner og fra håndtering av uønskede hendelser i disse virksomhetene.

forskrift om sikkerhetsadministrasjon § 2-1, 1. ledd *– om ansvar for sikkerhetstjenesten i underlagte virksomheter*
forskrift om sikkerhetsadministrasjon § 2-2, 1. ledd *– om ansvar overfor private leverandører*
forskrift om sikkerhetsadministrasjon § 2-6 *– om ansvar for sikkerhet ifm. anskaffelser*

Arbeidsoppgaver utført av andre virksomheter, herunder hos underlagte virksomheter, må omfattes av sikkerhetsrevisjoner.

Andre virksomheter som utfører arbeidsoppgaver med betydning for sikkerhet må utøve forebyggende sikkerhetstjeneste, og herunder gjennomføre egne sikkerhetsrevisjoner. Informasjon om resultater fra disse må være tilgjengelig for virksomheten. I tillegg bør virksomheten i nødvendig grad selv gjennomføre sikkerhetsrevisjoner hos andre virksomheter.

Tilsvarende gjelder overfor underordnede virksomheter.

Også leverandører i sikkerhetsgraderte anskaffelser må utøve forebyggende sikkerhetstjeneste og herunder gjennomføre egne sikkerhetsrevisjoner. I tillegg må anskaffelsesmyndigheten jevnlig, minimum hver 18. måned, kontrollere leverandørens forebyggende sikkerhetstjeneste.

Leverandøravtale må omfatte vilkår som gir NSM rett til å gjennomføre undersøkelser hos leverandøren i forbindelse med tilsyn med virksomheten.

sikkerhetsloven § 27, 2. ledd, litra b *– om avtalevilkår ifm. undersøkelser og kontroll hos leverandør*
forskrift om sikkerhetsadministrasjon § 2-1, 1. ledd *– om ansvar for sikkerhetstjenesten i underlagte virksomheter*
forskrift om sikkerhetsadministrasjon § 2-2, 1. ledd *– om ansvar overfor private leverandører*
forskrift om sikkerhetsadministrasjon § 2-6 *– om ansvar for sikkerhet ifm. anskaffelser*
Ytterligere bestemmelser er gitt i ***forskrift om sikkerhetsgraderte anskaffelser.***

Virksomheter må utveksle informasjon om uønskede hendelser og samarbeide om korrigering av slike hendelser.

Informasjon om uønskede hendelser må meddeles andre som hendelsen kan få betydning for, herunder må:

- kompromittering av sikkerhetsgradert informasjon rapporteres til informasjonens utsteder og til andre kompromitteringen kan ha betydning for
- utsteder meddeles dersom mottaker av sikkerhetsgradert informasjon vurderer at informasjonen ikke har riktig sikkerhetsgradering
- avsender informeres om (mulig) kompromittering av kurerpost

Berørte virksomheter må i nødvendig grad samarbeide om korrigering av uønskede hendelser. Utsteder av sikkerhetsgradert informasjon må ved kompromittering redegjøre for tiltak som kan begrense skade. Ved kompromittering må mottaker og avsender av kurerpost samarbeide om undersøkelser og gjennomføring av tiltak.

forskrift om sikkerhetsadministrasjon § 5-5 *– om rapportering mellom virksomheter*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

7 Sikkerhetsdokumentasjon

Dette kapittelet gir veiledning i regelverkets bestemmelser om dokumentering av den forebyggende sikkerhetstjenesten, det vil si om styrende, utførende og kontrollerende sikkerhetsdokumenter.

Beslutninger og føringer, ansvars- og myndighetsforhold, gjennomføring og erfaringer knyttet til forebyggende sikkerhetstjeneste må være sporbare, etterprøvbare og kjent for alle med tjenestlig behov. Dette innebærer at den forebyggende sikkerhetstjenesten må dokumenteres.

Korrekt, tilstrekkelig og tilgjengelig sikkerhetsdokumentasjon er en forutsetning for å skape tillit til, og mulighet for kontroll av, sikkerhetstjenesten.

7.1 Styrende, utførende og kontrollerende dokumenter

De beslutninger og føringer som ligger til grunn for den forebyggende sikkerhetstjenesten må beskrives i styrende dokumenter.

Styrende sikkerhetsdokumenter må utformes slik at de synliggjør den forebyggende sikkerhetstjenesten og slik bidra til at det skapes tillit til at nødvendig beskyttelse oppnås. Styrende dokumentasjon må omfatte beskrivelser av:

- hvilken sikkerhetsgradert informasjon virksomheten behandler, eksempelvis gjennom angivelse av virksomhetens autorisasjon for behandling av sikkerhetsgradert informasjon
- hvilke klassifiserte objekter virksomheten råder over
- fordeling av utøvende ansvar og myndighet for arbeidsoppgaver med betydning for sikkerheten, eksempelvis i form av organisasjonskart, stillingsbeskrivelser eller arbeidsinstrukser
- fordeling av utøvende ansvar og myndighet for utførende og kontrollerende sikkerhetsoppgaver, eksempelvis i form av funksjonsbeskrivelser for sikkerhetsorganisasjonen
- fysiske områder i virksomheten hvor sikkerhetsgradert informasjon kan behandles, med angivelse av graderingsnivå, eksempelvis i form av romplan
- informasjonssystemer i virksomheten som kan benyttes for håndtering av sikkerhetsgradert informasjon med angivelse av graderingsnivå og kommunikasjonsforbindelser, eksempelvis i form av konfigurasjonskart og utstyrsregister
- ansvars- og myndighetsfordeling overfor andre virksomheter, eksempelvis i form av avtaler med leverandører og med samarbeidspartnere
- krav til, og plan for vedlikehold av, kompetanse, eksempelvis i stillingsbeskrivelser, arbeidsinstrukser, funksjonsbeskrivelser, og i form av kompetanseplan
- oppfølging av den forebyggende sikkerhetstjenesten, eksempelvis i form av plan for interne sikkerhetsrevisjoner (revisjonsprogram)

sikkerhetsloven § 1 *– om forebyggende sikkerhetstjeneste som gir grunnlag for tillit*
sikkerhetsloven § 5, 3. ledd *– om skriftlig delegasjon av utøvende funksjoner i de forebyggende sikkerhetstjenesten*
sikkerhetsloven § 27 *– om inngåelse av sikkerhetsavtale ved sikkerhetsgraderte anskaffelser*
forskrift om sikkerhetsadministrasjon § 2-6, 3. ledd *– om avtale mellom virksomheter tilkoblet felles informasjonssystem*
forskrift om sikkerhetsadministrasjon § 3-3 *– om grunnlagsdokument for sikkerhet*
forskrift om sikkerhetsadministrasjon § 3-5 *– om stillingsbeskrivelse og arbeidsinstruks*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet*** *og i* ***forskrift om sikkerhetsgraderte anskaffelser.***

Utførelse av arbeidsoppgaver med betydning for sikkerhet må beskrives i utførende dokumenter.

Utførende sikkerhetsdokumenter må utformes slik at arbeidsoppgaver med betydning for sikkerhet utføres riktig og likt hver gang de repeteres, og slik bidra til at det skapes tillit til at nødvendig beskyttelse oppnås. Utførende dokumentasjon må omfatte beskrivelser av:

- generelle sikkerhetstiltak og grunnleggende forholdsregler, eksempelvis i form av sikkerhetsinstruks og beskrivelse av taushetsplikt (taushetserklæring)
- tiltak og forholdsregler knyttet til konkrete arbeidsoppgave eller situasjoner, eksempelvis i form av sikkerhetsbestemmelser i arbeidsrutiner, eller (rene) sikkerhetsprosedyrer
- sikkerhetstiltak, eksempelvis i form av beskrivelse av innstilling og funksjon for tekniske tiltak

sikkerhetsloven § 1 *– om forebyggende sikkerhetstjeneste som gir grunnlag for tillit*
forskrift om sikkerhetsadministrasjon § 3-3, 2. ledd, 6. pkt. *– om grunnlagsdokument for sikkerhet*
forskrift om sikkerhetsadministrasjon § 3-4, *– om instrukser, prosedyrer og lister*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Resultater fra utøvelse av forebyggende sikkerhetstjeneste må registreres i kontrollerende dokumenter.

Kontrollerende sikkerhetsdokumenter må utformes slik at utøvelse av forebyggende sikkerhetstjeneste er sporbar og kan kontrolleres. Kontrollerende dokumentasjon må omfatte:

- beslutninger etter ledelsens evaluering av sikkerhetstilstanden
- resultater fra interne sikkerhetsrevisjoner
- håndtering av uønskede hendelser
- registreringer av kompetanse og gjennomført opplæring
- registreringer fra behandling av sikkerhetsgradert informasjon og fra bruk av sikkerhetsgraderte informasjonssystemer
- registreringer ved utførelse av sikkerhetsprosedyrer og -tiltak

sikkerhetsloven § 1 *– om forebyggende sikkerhetstjeneste som gir muligheter for kontroll*
forskrift om sikkerhetsadministrasjon § 3-2, 3. ledd *– om registrering av opplæring*
forskrift om sikkerhetsadministrasjon § 4-4, 3.ledd *– om dokumentering sikkerhetsrevisjon og ledelsens gjennomgang*
forskrift om sikkerhetsadministrasjon § 5-2 *– om skadevurdering*
forskrift om sikkerhetsadministrasjon § 5-4, 2. ledd *– om registrering av sikkerhetstruende hendelser*
forskrift om sikkerhetsadministrasjon § 5-6, 1. – 3. ledd *– foreløpig rapport, utfyllende rapport, endelig rapport*
Ytterligere bestemmelser er gitt i ***forskrift om personellsikkerhet*** *og i* ***forskrift om informasjonssikkerhet.***

7.2 Sikkerhetsinstruks

Sikkerhetsinstruks for forebyggende sikkerhetstjeneste må utarbeides og gjøres kjent for personellet.

Sikkerhetsinstruksen må beskrive hvordan personellet er ment å oppfylle sin plikt til å bidra til forebyggende sikkerhetstjeneste og herunder angi de grunnleggende forholdsregler og de generelle sikkerhetstiltak den enkelte må ivareta. Sikkerhetsinstruksen må omfatte:

- beskrivelse av formålet med den forebyggende sikkerhetstjenesten, herunder hvilke uønskede hendelser som må forhindres
- retningslinjer for vurdering og håndtering av risiko

- angivelse av tjenstlig behov, sikkerhetsklarering og autorisasjon som forutsetninger for tilgang til sikkerhetsgradert informasjon
- grunnkrav for håndtering av sikkerhetsgradert informasjon med angivelse av hvor slik informasjon kan håndteres, samt regler for medbringelse og forsendelse av slik informasjon
- grunnkrav for bruk av sikkerhetsgraderte informasjonssystemer, herunder regler kommunikasjon av slik informasjon
- grunnkrav for håndtering av klassifiserte objekter
- beskrivelse av handlinger i beredskapssituasjoner, herunder regler for varsling i virksomheten
- beskrivelse av handlinger ved uønskede hendelser, herunder regler for rapportering i virksomheten
- angivelse av følger, for virksomheten og den for personellet, dersom sikkerhetsinstruksen eller andre sikkerhetsbestemmelser, brytes

Sikkerhetsinstruksen kan samordnes med beskrivelse av taushetsplikt/taushetserklæring.

merknad: I virksomheter som benytter sikkerhetsgraderte informasjonssystemer i stort omfang, kan det være nødvendig å utarbeide egen datasikkerhetsinstruks.

sikkerhetsloven § 5, 2. ledd, litra a *– om utarbeidelse av sikkerhetsinstruks*
forskrift om sikkerhetsadministrasjon § 2-2, 2. ledd *– om veiledning av underordnede*
forskrift om sikkerhetsadministrasjon § 3-1, 2. ledd *– om veiledning og til tilgang til sikkerhetsbestemmelser*

7.3 Grunnlagsdokument for sikkerhet

Grunnlagsdokument for sikkerhet må identifisere styrende og utøvende sikkerhetsdokumenter.

Virksomhetens grunnlagsdokument for sikkerhet må identifisere grunnleggende forutsetninger for behandlingen av skjermingsverdig informasjon, det vil si beskrive sikkerhetsdokumentasjonens oppbygging, identifisere styrende og utførende sikkerhetsdokumenter og anvise tilgang til disse dokumentene.

merknad: I mindre virksomheter kan det være aktuelt å samle alle styrende og utøvende sikkerhetsdokumenter ett sted. Denne samlingen utgjør da virksomhetens grunnlagsdokument for sikkerhet,

forskrift om sikkerhetsadministrasjon § 3-3 *– om grunnlagsdokument for sikkerhet*

7.4 Håndtering av sikkerhetsdokumentasjon[12]

Sikkerhetsdokumenter må sikkerhetsgraderes i forhold til skade som kan oppstå dersom innholdet blir kjent for uvedkommende.

Styrende, utførende og kontrollerende sikkerhetsdokumenter må sikkerhetsgraderes i forhold til skade det kan få om informasjon om utøvelsen av forebyggende sikkerhetstjeneste blir kjent for uvedkommende.

Informasjon om forebyggende sikkerhetstjeneste må i nødvendig grad være kjent for egne medarbeidere og for innleide. Også personer utenfor virksomheten vil i enkelte situasjoner få informasjon om sikkerhetstiltak og -prosedyrer, eksempelvis besøkende som informeres om

[12] For arkivverdige sikkerhetsdokumenter gjelder også arkivlovens bestemmelser.

adgangsprosedyrer. Sikkerhetsdokumenter må følgelig utformes og sikkerhetsgraderes slik at dokumentasjonen er tilgjengelig for dem de gjelder.

sikkerhetsloven § 11 *– om sikkerhetsgradering av informasjon*
forskrift om sikkerhetsadministrasjon § 3-1, 2. ledd *– om kjennskap til sikkerhetsbestemmelser*
Ytterligere bestemmelser er gitt i ***forskrift om personellsikkerhet*** *og i* ***forskrift om informasjonssikkerhet.***

Utarbeidelse og distribusjon av sikkerhetsdokumenter må være systematisk og sporbar.

Sikkerhetsdokumenter må til enhver tid være autoritative, korrekte og tilgjengelige for dem de gjelder. Utarbeidelse, godkjenning, distribusjon og tilbaketrekking av sikkerhetsdokumenter må derfor være styrt. Dokumentstyringen må angi myndighet for utgivelse av sikkerhetsdokumenter, samt sikre at dokumenter er tilgjengelig for alle som har behov for dem eksempelvis gjennom registrering av fordeling, kvittering eller lignende.

sikkerhetsloven § 5, 2. ledd, litra a og 3. ledd *– om ansvar for utarbeidelse av sikkerhetsinstruks*
forskrift om sikkerhetsadministrasjon § 3-1, 2. ledd *– om kjennskap til sikkerhetsbestemmelser*
forskrift om sikkerhetsadministrasjon § 3-4 *– om instrukser, rutiner og prosedyrer*
forskrift om sikkerhetsadministrasjon § 3-5 *– om stillingsbeskrivelser og arbeidsinstrukser*

Sikkerhetsdokumenter må oppbevares over tid.

Uønskede hendelser oppdages ikke alltid samtidig med at de oppstår. Sikkerhetsdokumenter må derfor oppbevares slik at det er mulig å gjenskape den forebyggende sikkerhetstjenesten på hendelsestidspunktet som grunnlag for undersøkelser. Sikkerhetsdokumenter må oppbevares lenge nok til at slike undersøkelser kan finne sted. Registreringer av sikkerhetstruende hendelser må oppbevares i minst 5 år.

Dokumentstyringen må omfatte bestemmelser om oppbevaring av sikkerhetsdokumenter.

sikkerhetsloven § 1 *– om forebyggende sikkerhetstjeneste som gir muligheter for kontroll*
Ytterligere bestemmelser er gitt i ***forskrift om personellsikkerhet*** *og i* ***forskrift om informasjonssikkerhet.***

8 Risiko

Dette kapittelet gir veiledning i regelverkets bestemmelser om risikohåndtering og risikovurdering.

Regelverkets bestemmelser om sikkerhetstiltak og -prosedyrer er minimumskrav. Virksomheten må selv avdekke behov for ytterligere tiltak og prosedyrer gjennom vurdering av den risiko sikkerhetsgradert informasjon eller klassifisert objekt faktisk er utsatt for.

Personellet må fortløpende vurdere om det er sikkert nok i en gitt situasjon å utføre arbeidsoppgaver som besluttet. Om nødvendig må personellet utøve risikohåndtering ved å forsterke beskyttelsen av skjermingsverdig informasjon eller objekt.

8.1 Grunnsikring og risikohåndtering

Sikkerhetstiltak og -prosedyrer må iverksettes i forhold til den risiko sikkerhetsgradert informasjon eller klassifisert objekt er utsatt for.

Regelverkets bestemmelser om sikkerhetstiltak og -prosedyrer er minimumskrav og angir således den grunnsikring som må etableres. Minimumskravene er basert på en generell risikovurdering i forhold til en vurdering av trusselnivået for Norge som helhet.

Behov for sikkerhetstiltak og -prosedyrer utover grunnsikringen må vurderes. Sikkerhetstiltak og -prosedyrer må iverksettes slik at faktiske risiko overfor sikkerhetsgradert informasjon eller klassifisert objekt håndteres. Herunder må risikovurderinger benyttes som grunnlag for:

- beskyttelse av systemer og utstyr i beskyttet område
- beskyttelse av informasjon om posisjon eller bevegelse av personer eller mobile enheter når slik informasjon anses som skjermingsverdig
- kravspesifikasjon for sikkerhet
- vurdering av tempestrisiko
- regulering av adgang og ferdsel i kontrollert område
- beskyttelse av sikkerhetsgradert informasjonssystem i utlandet
- beskyttelse av rom som er sikret, permanent eller midlertidig, mot avlytting og innsyn

sikkerhetsloven § 3, 1. ledd, nr. 1 *– forebyggende sikkerhetstjeneste definert*
sikkerhetsloven § 17 b *– om beskyttelse av skjermingsverdig objekt i forhold til klassifisering*
forskrift om sikkerhetsadministrasjon § 4-1 *– om risikohåndtering*
forskrift om sikkerhetsadministrasjon § 4-2, 3. ledd *– om personellets vurdering av risiko ved utførelse*
forskrift om sikkerhetsadministrasjon § 4-3 *– om gjennomføring og korrigering av sikkerhetstiltak*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Personellet må fortløpende vurdere om pålagte arbeidsoppgaver kan utføres sikkert nok og være forberedt på situasjoner med endringer i risiko.

Personellet må gjennomføre sikkerhetstiltak og -prosedyrer som besluttet. Utover dette må personellet fortløpende vurdere om det er sikkert nok i en gitt situasjon å utføre arbeidsoppgaver som forutsatt.

Ved behov må personellet utøve risikohåndtering ved å iverksette ytterligere sikkerhetstiltak og -prosedyrer, samt be om veiledning. Eksempelvis kan det i enkelte situasjoner være nødvendig å benytte sikrere kommunikasjonsmidler enn det som opprinnelig er besluttet.

forskrift om sikkerhetsadministrasjon § 4-2, 3. ledd *– om risikohåndtering ved utførelse av aktiviteter*

8.2 Risikovurdering

Risikovurderinger må omfatte interne og eksterne forhold som kan påvirke sikkerhet og gjennomføres ved endringer av slike forhold.

Risiko uttrykkes som kombinasjonen av sannsynlighet for og konsekvens av at uønskede hendelser inntreffer.

Risikovurderinger må gjennomføres når interne eller eksterne forhold med betydning for sikkerhet oppstår eller endres.

Risikovurderinger må ha som mål å avdekke behov for sikkerhetstiltak og prosedyrer utover regelverkets minimumskrav, avdekke overflødige og unødvendig overlappende tiltak og prosedyrer og finne frem til mer kosteffektive tiltak og prosedyrer som erstatning for eksisterende.

sikkerhetsloven § 3, 1. ledd, nr. 1 *– forebyggende sikkerhetstjeneste definert*
forskrift om sikkerhetsadministrasjon § 4-2, 2. ledd *– om kontinuerlig risikovurdering*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

Risikovurderinger må omfatte vurdering av sannsynlighet for uønsket hendelse.

Sannsynlighetsvurderingen utføres med utgangspunkt i kunnskap om sårbarheter og om de sikkerhetstiltak og -prosedyrer som er ment å motvirke disse. Sannsynlighetsvurderingen kan gjennomføres ved å betrakte hva som skal til for å forårsake en uønsket hendelse, eksempelvis:

- Vurdering av om uønskede hendelser kan forårsakes gjennom tilfeldigheter (uaktsomt), gjennom bevisste handlinger (forsett) eller om plan og forberedelse må til (overlegg). Hendelser som kan forårsakes uaktsomt er da mer sannsynlige enn de som krever forsett eller til og med overlegg.
- Vurdering av om kompetanse og ressurser må til for å forårsake uønskede hendelser. Hendelser som kan forårsakes uten særlig kompetanse og uten hjelpemidler er da mer sannsynlige enn de som krever sikkerhetsfaglig kompetanse, kunnskaper om den forebyggende sikkerhetstjenesten og tekniske hjelpemidler.
- Vurdering av om sikkerhetstiltak eller -prosedyrer i tilstrekkelig grad er iverksatt for å hindre uønsket hendelse. Hendelser som ikke hindres er da mer sannsynlige enn de som hindres gjennom flere uavhengige sikkerhetstiltak og -prosedyrer.

forskrift om sikkerhetsadministrasjon § 4-2, 2. ledd *– om risikovurdering*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet?***

Risikovurderinger må omfatte vurdering av konsekvens av uønsket hendelse.

Konsekvensvurderingen er på overordnet nivå sammenfallende med vurderingen av den skade som kan oppstå når sikkerhetsgradert informasjon[13] eller klassifisert objekt ikke er tilstrekkelig beskyttet.

sikkerhetsloven § 11 *– om sikkerhetsgradering av informasjon*
sikkerhetsloven §§ 17 og 17b *– om klassifisering av skjermingsverdig objekt*
Ytterligere bestemmelser er gitt i ***forskrift om informasjonssikkerhet.***

[13] Veiledning om vurdering av skade som følge av at skjermingsverdig blir tilgjengelig for uvedkommende er gitt i Nasjonal sikkerhetsmyndighets "Veiledning i verdivurdering".

9 Vedlegg A – Dokumenthistorie

2010-07-01 1.0 Gjeldende versjon