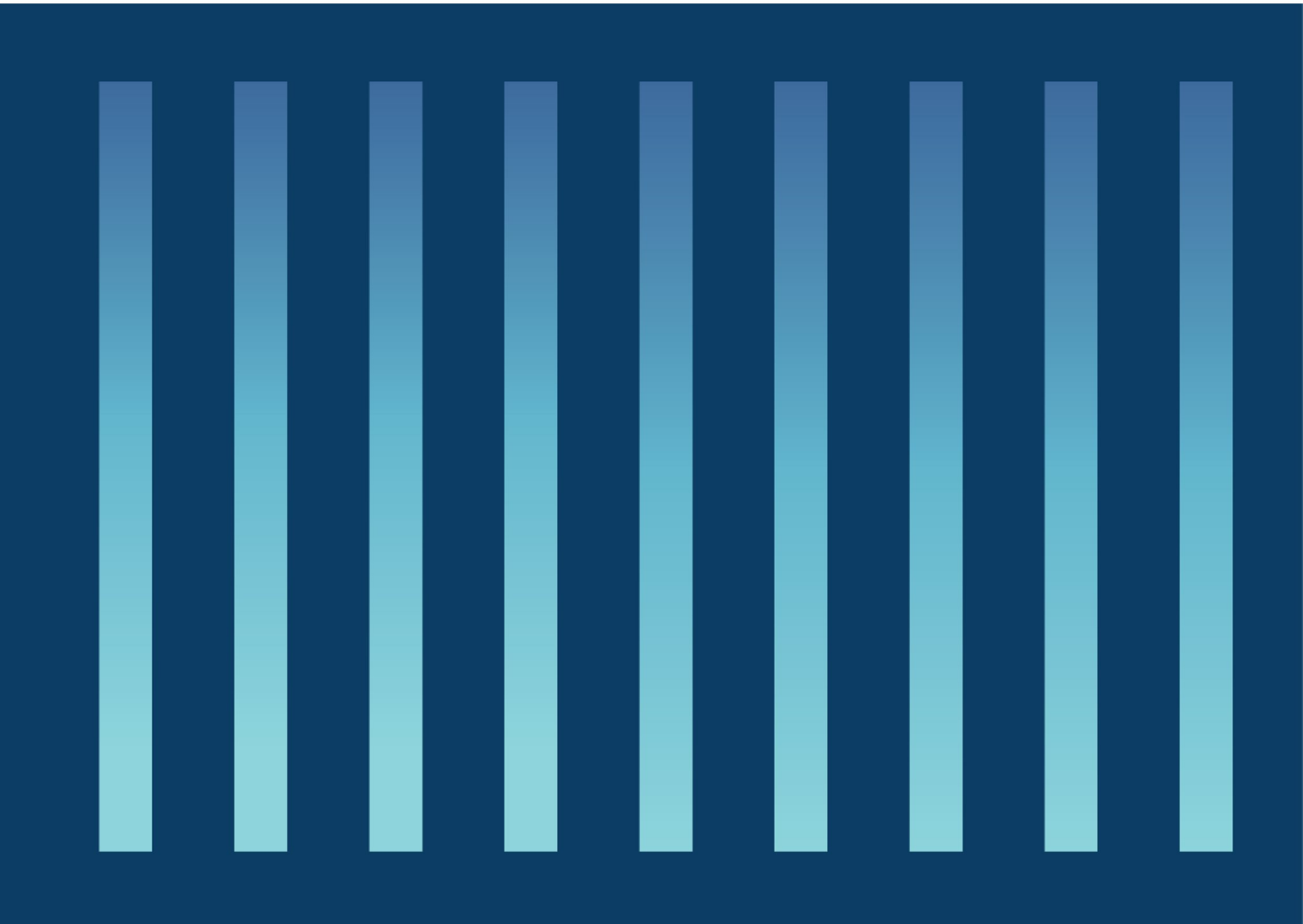
NASJONAL
SIKKERHETSMYNDIGHET

Veileder for tilsyn med forebyggende sikkerhetsarbeid

Versjon: 2



Nasjonal sikkerhetsmyndighet (NSM) er fagorgan for forebyggende sikkerhet, og sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven). NSM skal gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid.

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019. Loven skal bidra til å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

Sikkerhetsloven gjelder for statlige, fylkeskommunale og kommunale organer og for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. De enkelte departementer skal innenfor sitt ansvarsområde vedta at andre virksomheter skal underlegges loven dersom de behandler sikkerhetsgradert informasjon eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for disse funksjonene.

NSMs veiledere utdyper regelverkforståelsen, herunder den tematiske sammenhengen mellom ulike bestemmelser i sikkerhetsloven og tilhørende forskrifter. Veilederne representerer NSMs syn på hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket.

NSM gir i tillegg ut håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen.

Veilederen anbefales lest i sammenheng med lov og forskrift, samt NSMs øvrige relevante veiledere, håndbøker og tekniske råd.

INNHOLD

1. Tilsyn 5
1.1. Tilsynsmyndigheter 5
1.1.1. Sektormyndighet med tilsynsansvar 5
1.1.2. Sikkerhetsmyndigheten 6
1.1.3. Samarbeid om tilsyn 6
1.1.4. Pålegg om gjennomføring av tilsyn 8
1.2. Tilsynsobjekter 8
2. Systemrevisjon 10
2.1. Tilsyn ved hjelp av systemrevisjon 10
3. IKT-revisjon 12
3.1. Tilsyn ved hjelp av IKT-revisjon 12
4. Planlegging og gjennomføring av tilsyn 13
4.1. Risikobasert tilsyn 13
4.1.1. Årlig tilsynsprogram 14
4.1.2. Tilsynsplan 14
4.2. Varsel 14
4.3. Gjennomføring 15
4.4. Rapportering 15
4.5. Opplysninger fra tilsyn 16
4.6. NSMs tilsynsmetodikk 17
5. Reaksjoner etter tilsyn 18
5.1. Pålegg 18
5.2. Tvangsmulkt 18
5.3. Overtredelsesgebyr 19
5.4. Politianmeldelse 20
6. Vedlegg A – Kriterier for forsvarlig sikkerhetsnivå 21
6.1. Scenarioer 21
6.2. Aktører 22
6.2.1. Tilhørighet 22
6.2.2. Kapasitet (eller evne) 22
6.2.3. Intensjon (eller vilje) 22
6.3. Tiltaksvurdering 22
6.3.1. Vurdering av tiltak for å beskytte skjermingsverdig informasjon 23
6.3.2. Vurdering tiltak for å beskytte skjermingsverdig objekt eller infrastruktur 24
7. Vedlegg B – Kriterier for sikkerhetsstyring 26
7.1. Sikkerhetsledelse 27

7.1.1. Ressurser og kompetanse 27
7.2. Sikkerhetsorganisering 28
7.2.1. Roller i det forebyggende sikkerhetsarbeidet 28
7.2.2. Taushetsplikt 29
7.2.3. Sikkerhet ved fratredelse 29
7.3. Sikkerhetstiltak og -prosedyrer 30
7.3.1. Beredskap 30
7.3.2. Prinsipper for valg av sikkerhetstiltak - og prosedyrer 31
7.4. Forholdet til andre virksomheter 31
7.5. Sikkerhetsoppfølging 32
7.5.1. Håndtering av uønskede hendelser 33
7.5.2. Evaluering av forebyggende sikkerhetsarbeid 33
7.5.3. Leders gjennomgang av forebyggende sikkerhetsarbeid 34
7.6. Sikkerhetsdokumentasjon 35
8. Vedlegg C – Kriterier for risikostyring 36
8.1. Risikostyring 36
8.2. Risikohåndtering 37
8.3. Avhengigheter 38

1. Tilsyn

Målgruppen for *Veileder for tilsyn med forebyggende sikkerhetsarbeid* er sektormyndigheter med tilsynsansvar, det vil si personell som skal føre tilsyn med virksomheter som er omfattet av sikkerhetsloven. Veilederen vil også være nyttig for personell hos tilsynsobjektene.

Tilsyn med forebyggende sikkerhetsarbeid er lovpålagt kontroll med at bestemmelser i sikkerhetsloven med forskrifter, etterleves. Overordnet formål er å skape tillit til det forebyggende sikkerhetsarbeidet og bidra til å redusere sårbarheter i en virksomhet, en sektor og i nasjonen som helhet. Tilsyn skal bidra til forbedring av virksomhetenes arbeid med forebyggende sikkerhet.

1.1. Tilsynsmyndigheter

Sikkerhetsloven fordeler ansvar og myndighet for tilsyn i:

> *§ 3-1. Tilsyn med virksomheter*
>
> *Sikkerhetsmyndigheten fører tilsyn med virksomheter som er omfattet av loven.*
>
> *Departementet kan bestemme at myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, skal føre tilsyn med virksomheter som er omfattet av loven. Sikkerhetsmyndigheten skal likevel gjennomføre tilsyn når det følger av internasjonale forpliktelser eller når det er tvingende nødvendig.*
>
> *Sikkerhetsmyndigheten skal føre tilsyn med departementene og myndigheter med tilsynsansvar etter andre ledd.*
>
> *Kongen kan gi forskrift om tildeling av tilsynsansvar og om fordeling av ansvaret mellom sikkerhetsmyndigheten og aktuelle myndigheter med sektoransvar.*

Tilsynsansvar er fordelt mellom sektormyndigheter med tilsynsansvar og sikkerhetsmyndigheten.

1.1.1. Sektormyndighet med tilsynsansvar

Et departement kan tildele en eksisterende sektormyndighet ansvar for å føre tilsyn med forebyggende sikkerhetsarbeid i sin sektor. Slik tildeling skjer etter en helhetsvurdering og i samarbeid med NSM. Tildeling forutsetter at sektormyndigheten:

- allerede har ansvar for å føre tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur
- har eller kan opparbeide seg nødvendig kompetanse for gjennomføring av tilsyn med at sikkerhetskrav i eller i medhold av sikkerhetsloven overholdes

Ved å gi eksisterende sektormyndigheter ansvar for tilsyn med forebyggende sikkerhetsarbeid sikres det at tilsynsmyndigheten har bransjekunnskap gjennom kunnskap om tilsynsobjektene i sektorlovgivningen. Bransjekunnskap betinger med andre ord samsvar mellom tilsynsansvaret i sektorlovgivningen og tilsynsansvaret for forebyggende sikkerhetsarbeid. Behovet for

bransjekunnskap kan medføre at departementer må tildele tilsynsmyndighet til flere sektormyndigheter. Dersom et departement ikke tildeler tilsynsansvar er NSM tilsynsmyndighet i sektoren.

1.1.2. Sikkerhetsmyndigheten

NSM er tilsynsmyndighet i alle sektorer der tilsynsansvaret ikke er lagt til en sektormyndighet. NSM kan føre tilsyn også i sektorer med egen tilsynsmyndighet, dersom det:

- følger av internasjonale forpliktelser, eksempelvis forpliktelser i avtaler med andre stater eller internasjonale organisasjoner om behandling av sikkerhetsgradert informasjon
- er tvingende nødvendig, eksempelvis når det foreligger konkrete sikkerhetsinteresser som ved sikkerhetstruende virksomhet og alvorlige sikkerhetsbrudd, eller ved mistanke eller kunnskap om aktivitet som kan innebære risiko overfor nasjonale sikkerhetsinteresser

I tillegg fører NSM tilsyn med sektormyndigheter med tilsynsansvar. Slike tilsyn omfatter, i tillegg til kontroll av forebyggende sikkerhetsarbeid, også undersøkelse av sektormyndighetens egen gjennomføring av tilsyn.

NSM fører tilsyn med departementer. Slike tilsyn omfatter, i tillegg til kontroll av forebyggende sikkerhetsarbeid, også undersøkelse av departementets utøvelse av ansvar for forebyggende sikkerhetsarbeid i egen sektor.

Sikkerhetsloven § 2-2 gir NSM sektorovergripende ansvar for forebyggende sikkerhetsarbeid. Dette ansvaret omfatter blant annet å se til at det føres tilsyn med at virksomheter oppfyller krav til forebyggende sikkerhetsarbeid, samt å utarbeide og vedlikeholde grunnleggende kriterier for tilsyn.

1.1.3. Samarbeid om tilsyn

Selv om tilsyn med forebyggende sikkerhetsarbeid gjennomføres av forskjellige tilsynsmyndigheter, NSM og sektormyndigheter med tilsynsansvar, skal tilsynet være enhetlig på tvers av sektorer. Dette forutsetter samarbeid mellom NSM og sektormyndighetene. Sikkerhetsloven har bestemmelser om slikt samarbeid i:

§ 3-2. Samarbeid mellom sikkerhetsmyndigheten og andre myndigheter med tilsynsansvar

Sikkerhetsmyndigheten og myndigheter med tilsynsansvar etter § 3-1 andre ledd skal inngå en avtale om samarbeid. Gjennomføring av tilsyn skal så langt det er mulig samordnes med andre tilsynsmyndigheter.

Sikkerhetsmyndigheten skal utarbeide og utvikle grunnleggende kriterier for tilsyn etter loven, og legge til rette for felles opplæring av tilsynspersonell.

Sikkerhetsmyndigheten kan om nødvendig medvirke til forberedelse og gjennomføring av tilsyn som utføres av myndigheter med tilsynsansvar. Myndigheter med tilsynsansvar kan be sikkerhetsmyndigheten om slik bistand.

Myndigheter med tilsynsansvar skal orientere sikkerhetsmyndigheten om planlagte tilsyn, redegjøre for gjennomførte tilsyn og informere om eventuelle avvik og pålegg.

Kongen kan gi forskrift om samarbeid og informasjonsutveksling mellom sikkerhetsmyndigheten og myndigheter med tilsynsansvar.

Utdypende krav til samarbeid fremgår av virksomhetsikkerhetsforskriften:

§ 90. Avtale om samarbeid mellom Nasjonal sikkerhetsmyndighet og andre myndigheter med tilsynsansvar

Overordnet departement til en sektormyndighet med tilsynsansvar, har ansvaret for at det inngås samarbeidsavtaler mellom Nasjonal sikkerhetsmyndighet og myndigheten med tilsynsansvar etter sikkerhetsloven § 3-2.

Det skal følge av slike samarbeidsavtaler

a) hvilke kriterier som skal ligge til grunn for tilsyn

b) hvem som skal være ansvarlig for opplæring og veiledning, og hvordan opplæring og veiledning skal gjennomføres

c) hvordan tilsyn der både Nasjonal sikkerhetsmyndighet og sektormyndigheten deltar, skal forberedes og gjennomføres

d) hvordan Nasjonal sikkerhetsmyndighet skal dele relevant informasjon om trusselbildet og risiko med sektormyndigheten

e) hvordan sektormyndigheten skal rapportere til Nasjonal sikkerhetsmyndighet om planlagte tilsyn

f) hvordan varslinger etter sikkerhetsloven § 4-5 skal behandles

g) hvordan godkjennings- og dispensasjonsmyndighet i sektoren skal utøves

h) hvordan sektormyndigheten skal dele kunnskap og erfaringer med Nasjonal sikkerhetsmyndighet.

Myndigheter som er tildelt tilsynsansvar etter sikkerhetsloven § 3-1, har ansvaret for tilsynet også når Nasjonal sikkerhetsmyndighet medvirker til eller deltar på tilsynet.

Samarbeid om tilsyn mellom NSM og sektormyndighet med tilsynsansvar skal nedfelles og formaliseres i en samarbeidsavtale. Kravet om samarbeidsavtale må forstås slik at avtaleinngåelsen er en forutsetning for etablering av sektormyndighet med tilsynsansvar. Departementet som tildeler tilsynsansvar, har ansvaret for at samarbeidsavtale inngås.

Samarbeidsavtalen skal omfatte vilkår for:

- *tilsynskriterier* – NSM har ansvar for utvikling av kriterier for tilsyn. Utviklingen skjer med bidrag fra sektormyndighetene og disse kan supplere NSMs tilsynskriterier med kriterier tilpasset den enkelte sektor. Kriterier for tilsyn med sentrale deler av sikkerhetsloven med forskrifter fremgår av vedlegg A – C[1].
- *kompetanse* – Sektormyndigheter med tilsynsansvar skal ha (eller kunne opparbeide seg) nødvendig kompetanse for gjennomføring av tilsyn med at sikkerhetskrav i eller i medhold av sikkerhetsloven overholdes. NSM skal bistå sektormyndigheten med opparbeiding og vedlikehold av kompetanse, eksempelvis i form av kurs eller deltagelse som observatør under tilsyn.
- *gjennomføring* – Sektormyndigheter med tilsynsansvar har selvstendig ansvar for gjennomføring av egne tilsyn, også tilsyn der NSM bistår eller deltar. Tilsynsmyndigheten skal

[1] Vedleggene beskriver kort de aktuelle bestemmelsene. Mer utfyllende veiledning fremgår av NSMs øvrige veiledere.

samordne tilsynene blant annet for å unngå unødig belastning for virksomhetene. NSM kan bistå ved gjennomføring av tilsyn, eksempelvis med fagspesifikke undersøkelser. NSM kan på bakgrunn av sikkerhetsfaglige vurderinger, kreve å delta på sektormyndighetenes tilsyn.

- *informasjonsdeling* –Tilsynsmyndighetene skal dele informasjon seg imellom. Eksempelvis skal informasjon om planlegging, gjennomføring og resultater av tilsyn deles mellom NSM og sektormyndighetene. NSM skal gi sektormyndighetene sektorovergripende informasjon, blant annet om trusler, sårbarheter og sikkerhetstiltak. Sektormyndighetene skal dele sektorspesifikk informasjon med betydning for forebyggende sikkerhetsarbeid med NSM.

NSM har utarbeidet mal for samarbeidsavtale. Videre har NSM etablert en arena for samhandling med og mellom sektormyndigheter med tilsynsansvar. Samhandlingsarenaen benyttes for videreutvikling av tilsynskriterier, opplæring av tilsynspersonell, planlegging og samordning av tilsyn og øvrig informasjonsdeling. Samhandlingsarenaen ledes av NSM og samtlige sektormyndigheter med tilsynsansvar deltar.

1.1.4. Pålegg om gjennomføring av tilsyn

NSM kan gi sektormyndigheter med tilsynsansvar pålegg om utførelsen av tilsyn i medhold av sikkerhetsloven:

> *§ 3-6. Pålegg (andre ledd)*
>
> *Dersom myndigheter med tilsynsansvar ikke fører tilsyn i samsvar med krav fastsatt i eller i medhold av loven, kan sikkerhetsmyndigheten gi pålegg om å utføre slikt tilsyn.*

Forhold knyttet til gjennomføring av tilsyn avklares normalt gjennom kontakt mellom NSM og sektormyndighetene med tilsynsansvar, typisk gjennom arbeidet i samhandlingsarenaen. NSM kan gi sektormyndigheten pålegg om gjennomføring av tilsyn. Slike pålegg kan være aktuelle når tilsyn ikke planlegges, gjennomføres eller følges opp i henhold til krav i sikkerhetsloven med forskrifter. Eksempelvis kan det være aktuelt dersom det ikke gjennomføres tilsyn i nødvendig omfang eller dersom fastlagt metode og kriterier ikke legges til grunn for tilsynene.

1.2. Tilsynsobjekter

Hvem sikkerhetsloven gjelder for fremgår av:

> *§1-2. Hvem loven gjelder for*
>
> *Loven gjelder for statlige, fylkeskommunale og kommunale organer.*
>
> *Loven gjelder for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser etter kapittel 9.*
>
> *For virksomheter på Svalbard, Jan Mayen og i bilandene gjelder loven i det omfang og med de stedlige tilpassinger kongen bestemmer.*
>
> *Kongen kan i statsråd gi forskrift om lovens virkeområde og helt eller delvis unna bestemte virksomheter eller visse typer informasjon, informasjonssystemer, objekter og infrastruktur.*

I tillegg fremgår det av sikkerhetsloven:

> *§1-3. Vedtak om at loven skal gjelde for andre virksomheter (første ledd)*
>
> *Et departement skal innenfor sitt ansvarsområde fatte vedtak om at loven helt eller delvis skal gjelde for virksomheter som*
>
> *a) behandler sikkerhetsgradert informasjon*
>
> *b) råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner*
>
> *c) driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner*

Sikkerhetsloven gjelder for[2]:

- statlige, fylkeskommunale og kommunale organer
- leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser
- virksomheter et departement har fattet vedtak om at loven skal gjelde for

Med statlige, fylkeskommunale og kommunale organer menes forvaltningsorganer iht. forvaltningsloven §1.

Det skal føres tilsyn med alle virksomheter omfattet av loven, jf:

> *§ 3-1. Tilsyn med virksomheter*
>
> *Sikkerhetsmyndigheten fører tilsyn med virksomheter som er omfattet av loven.*
>
> *Departementet kan bestemme at myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur, skal føre tilsyn med virksomheter som er omfattet av loven. Sikkerhetsmyndigheten skal likevel gjennomføre tilsyn når det følger av internasjonale forpliktelser eller når det er tvingende nødvendig.*

Tilsyn gjennomføres for å undersøke, og ev. pålegge korrigering av det forebyggende sikkerhetsarbeidet i virksomheter underlagt sikkerhetsloven. Hensikten er således å bidra til å redusere sårbarheter og bistå i arbeid med forbedring av sikkerhetsarbeidet.

I tillegg bidrar tilsyn til å danne grunnlag for departementers utøvelse av ansvar for forebyggende sikkerhetsarbeid i egen sektor, jf. sikkerhetsloven § 2-1 og for NSMs sektorovergripende ansvar for forebyggende sikkerhetsarbeid, jf. sikkerhetsloven § 2-2.

[2] Sikkerhetslovens gyldighet på Svalbard, Jan Mayen og i bilandene, samt lovens anvendelse overfor Stortinget, Stortingets organer, regjeringen og dostolene som beskrevet i § 1-4, omhandles beskrives ikke nærmere i denne veilederen.

2. Systemrevisjon

Systemrevisjon er en systematisk undersøkelse av et styringssystem for å avgjøre om det oppfyller fastlagte kriterier[3] og fungerer etter hensikten. Systemrevisjon gjennomføres med andre ord for å identifisere eventuelle mangler ved styringssystemet som grunnlag for korrigering og forbedring.

2.1. Tilsyn ved hjelp av systemrevisjon

Sikkerhetsloven § 3-4 bestemmer at det gis forskrift om stedlig tilsyn. Av virksomhetsikkerhetsforskriften fremgår det at tilsyn som hovedregel skal gjennomføres som systemrevisjon:

> *§ 89. Tilsyn med virksomheter underlagt lov om nasjonal sikkerhet (tredje ledd)*
>
> *Tilsyn skal som hovedregel gjennomføres som systemrevisjon.*

Forebyggende sikkerhetsarbeid skal gjennomføres planlagt og systematisk i form av sikkerhetsstyring, jf. sikkerhetsloven § 4-1. Det er i første rekke styringssystemet for sikkerhet som undersøkes ved tilsyn. De forebyggende sikkerhetstiltakene som utgjør dette styringssystemet skal dimensjoneres i forhold til risiko, jf. sikkerhetsloven § 4-2. Systemrevisjonene må derfor også omfatte undersøkelser av risikovurdering og -håndtering, det vil si av risikostyringen.

Systemrevisjoner gjennomføres ikke for å avdekke enkeltfeil, men som grunnlag for å vurdere styringssystemets samsvar og hensiktsmessighet. I den grad enkeltfeil avdekkes skal slike alltid håndteres.

I systemrevisjoner registreres revisjonsbevis. Dette er objektive fakta om det forebyggende sikkerhetsarbeidet. Revisjonsbevisene vurderes i sammenheng for å identifisere underliggende årsaker i form av mangler ved grunnprinsippene i sikkerhetsstyringen:

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

I tillegg må eventuelle mangler i risikostyringen identifiseres.

Manglene angis som avvik fra krav i sikkerhetsloven med forskrifter. Revisjonsbevis som ikke gir grunnlag for avvik kan angis som observasjoner som virksomheten må være oppmerksom på slik at disse ikke utvikler seg til avvik.

[3] Kriterier for systemrevisjon ved tilsyn med forebyggende sikkerhetsarbeidet fremgår av vedlegg A - C

Eksempel på vurdering av revisjonsbevis

Enkeltfeil ved at dør står åpen registreres som revisjonsbevis. I utgangspunktet kan dette vurderes som utilstrekkelig fysisk sikring, dvs. som en mangel knyttet til sikkerhetstiltak og -prosedyrer.

Etter andre undersøkelser er det imidlertid registrert som revisjonsbevis at flere medarbeidere ikke har gjennomført opplæring i fysisk sikring, dvs. en mangel knyttet til sikkerhetsorganisering.

Ytterligere undersøkelser har registrert som revisjonsbevis at virksomhetens ledelse har redusert opplæringen av nyansatte. Dette er en mangel knyttet til sikkerhetsledelse. Denne mangelen vurderes som underliggende årsak og angis som avvik.

Avvik skal håndteres ved å implementere varige, korrigerende tiltak som hindrer at avviket gjenoppstår. Gjentagelse hindres gjennom korrigering av avvikets underliggende årsaker. Slik korrigering forutsetter analyse av underliggende årsaker til avviket samt av om tilsvarende avvik har inntruffet tidligere eller andre steder i virksomheten.

Tilsyn med forebyggende sikkerhetsarbeid kan med fordel gjennomføres i henhold til anerkjente standarder for systemrevisjon som NS-EN ISO 19011 retningslinjer for revisjon av ledelsessystemer.

3. IKT-revisjon

IKT-revisjon er en systematisk undersøkelse av sikkerhet i, og ved bruk av informasjonssystemer. Systemrevisjon gjennomføres med andre ord for å identifisere eventuelle mangler ved informasjons- og informasjonssystemsikkerhet.

3.1. Tilsyn ved hjelp av IKT-revisjon

Sikkerhetsloven har bestemmelser om beskyttelse av informasjon og informasjonssystemer i kapitlene 5 og 6, og tilsyn må følgelig også omfatte disse bestemmelsene. Virksomhetsikkerhetsforskriften angir metode for kontroll av sikkerhetstilstanden i informasjonssystemer i:

> *§ 89. Tilsyn med virksomheter underlagt lov om nasjonal sikkerhet (fjerde ledd)*
>
> *For å kontrollere sikkerhetstilstanden til informasjonssystemer og infrastruktur, kan tilsynsmyndigheten benytte automatiserte metoder for å samle inn teknisk informasjon.*

Tilsyn med bestemmelser om beskyttelse av informasjon og informasjonssystemer kan gjennomføres som IKT-revisjon. Aktuelle revisjonskriterier er NSMs grunnprinsipper for IKT-sikkerhet og NS-EN ISO 27001/27002.

IKT-revisjon kan også omfatte automatiserte metoder for innsamling av teknisk informasjon. Automatiserte metoder kan eksempelvis være dataprogrammer eller applikasjoner som på selvstendig grunnlag samler inn informasjon om forhold av betydning for sikkerhetstilstanden i et informasjonssystem.

4. Planlegging og gjennomføring av tilsyn

For å sikre at tilsyn blir gjennomført ofte nok og i stort nok omfang, og med tilstrekkelige ressurser, skal tilsyn planlegges.

4.1. Risikobasert tilsyn

Virksomhetsikkerhetsforskriften har bestemmelser om planlegging av tilsyn i:

> *§ 3-2. Samarbeid mellom sikkerhetsmyndigheten og andre myndigheter med tilsynsansvar, fjerde ledd:*
>
> *Myndigheter med tilsynsansvar skal orientere sikkerhetsmyndigheten om planlagte tilsyn, redegjøre for gjennomførte tilsyn og informere om eventuelle avvik og pålegg.*

… og i:

> *§ 89. Tilsyn med virksomheter underlagt lov om nasjonal sikkerhet (andre ledd)*
>
> *Et tilsyn skal planlegges på bakgrunn av risiko og vesentlighet. Det skal gjennomføres tilsyn ofte nok og i stort nok omfang til at lovens formål ivaretas.*

Tilsynsobjekter og -omfang skal velges i forhold til betydning for nasjonale sikkerhetsinteresser etter vurdering av:

- *risiko* – med utgangspunkt i de verdier som skal beskyttes, trusler overfor disse verdiene og sårbarheter i denne beskyttelsen
- *vesentlighet* – med utgangspunkt i verdienes betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser

Informasjon til grunnlag for slike vurderinger kan være om:

- (mulige) uønskede hendelser (sikkerhetstruende virksomhet, sikkerhetsbrudd eller avvik)
- endringer som berører forebyggende sikkerhetsarbeid (internt, eksempelvis i forebyggende sikkerhetsarbeid – eller eksternt, i trusler eller regelverk)
- (endringer i) avhengigheter som berører det forebyggende sikkerhetsarbeidet

Hvert enkelt tilsyn skal planlegges. Kravet i § 3-2 må forstås slik at tilsynsmyndigheten også skal utarbeide en samlet plan for de tilsyn som skal utføres gjennom året. En slik årlig plan vil danne grunnlag for tilsynsmyndighetens egne tilsynsaktiviteter og samtidig være nødvendig for NSMs utøvelse av sitt sektorovergripende ansvar.

4.1.1. Årlig tilsynsprogram

Samlet plan for årlige tilsyn utformes som årlig tilsynsprogram som angir hvilke tilsyn som skal gjennomføres beskrevet ved:

- *tilsynsobjekt* – virksomheten det skal føres tilsyn med
- *tilsynsomfang* – hvilke deler av det forebyggende sikkerhetsarbeidet som skal undersøkes (organisasjonsledd, funksjon, sikkerhetsfag …)
- *tidspunkt* – for gjennomføring (av feltarbeid ved stedlig tilsyn, av undersøkelser i andre tilsynsformer)
- *revisjonslag* – med utpeking av revisjonsleder og ev. fagrevisorer og –eksperter

4.1.2. Tilsynsplan

Gjennomføring av det enkelte tilsyn planlegges med angivelse av tidspunkt for forberedelse (dokumentasjonsgjennomgang), feltarbeid (åpningsmøte, undersøkelser og sluttmøte) og rapportering.

I tillegg planlegges tilsynet i detalj med angivelse av tidspunkt, sted og deltagere for det enkelte intervju eller kontroll. Detaljert tilsynsplan utarbeides i samarbeid mellom tilsynsobjekt og tilsynsmyndighet i tiden mellom varsel og til feltarbeidet starter.

4.2. Varsel

Sikkerhetsloven har krav om varsling av tilsyn i:

> *§ 3-4. Adgangsrett og varslingsplikt ved stedlige tilsyn (annet ledd)*
>
> *Stedlige tilsyn skal varsles skriftlig. Tilsyn kan likevel gjennomføres uten varsel dersom sikkerhetshensyn gjør det nødvendig.*

Som hovedregel skal alle tilsyn varsles i forkant av gjennomføringen. Tilsynsvarselet skal angi tilsynshjemmelen sammen med tilsynsobjektets plikter og rettigheter i forbindelse med tilsynet. Varselet skal også angi hvilke dokumenter tilsynsobjektet skal oversende for dokumentgjennomgang som forberedelse til feltarbeid.

Tilsyn kan gjennomføres med kort eller ingen varslingstid dersom varsling ikke er mulig eller ønskelig som ved enkelte tilsyn i forbindelse med uønskede hendelser, eller når varsling vil kunne påvirke formålet med tilsynet.

4.3. Gjennomføring

Sikkerhetsloven har bestemmelser om gjennomføring i:

> *§ 3-3. Generelle prinsipper for tilsyn (første ledd)*
>
> *Tilsyn etter § 3-1 skal ikke forstyrre tilsynsobjektenes daglige drift mer enn nødvendig.*

Tilsynsmyndighetens adgangsrett og tilgang er regulert i:

> *§ 3-4. Adgangsrett og varslingsplikt ved stedlige tilsyn (første ledd)*
>
> *Tilsynsmyndigheten kan kreve tilgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur. Virksomheten skal stille med relevant personell under tilsynet så langt det er nødvendig.*

Stedlig tilsyn bør gjennomføres i form av feltarbeid som omfatter:

- *åpningsmøte* – med informasjon om tilsynet og endelig fastlegging av den detaljerte tilsynsplanen
- *feltarbeid* – som omfatter undersøkelser i form av intervjuer og kontroller
- *sluttmøte* – med avklaring av revisjonsbevis og informasjon om videre saksgang

Andre tilsynsformer vil typisk være avgrenset til gjennomføring av undersøkelser i form av gjennomgang av innsendt dokumentasjon. Feltarbeidets (undersøkelsenes) resultat er revisjonsbevis som tilsynsobjektet (i hovedsak) er enig i.

Tilsynsmyndigheter skal gis nødvendig adgang til tilsynsobjektet og nødvendig tilgang til personell for effektiv gjennomføring av tilsynet.

4.4. Rapportering

Virksomhetsikkerhetsforskriften har krav om rapportering av tilsyn i:

> *§ 91. Rapport etter tilsyn*
>
> *Etter et gjennomført tilsyn skal tilsynsmyndigheten utarbeide en foreløpig rapport som forelegges virksomheten for uttalelse. Det skal deretter utarbeides en endelig rapport som skal sendes til virksomheten og Nasjonal sikkerhetsmyndighet. Nasjonal sikkerhetsmyndighet kan gjøre endelige tilsynsrapporter tilgjengelige for Politiets sikkerhetstjeneste.*

Resultater fra tilsyn oppsummeres i en tilsynsrapport. Rapportutkastet oversendes tilsynsobjektet for kommentarer til revisjonsbevis, vurderingene av revisjonsbevisene og de avvik eller observasjoner som er resultater av disse vurderingene.

Etter at tilsynsmyndigheten har mottatt og vurdert tilsynsobjektets kommentarer, utarbeides endelig tilsynsrapport. Denne oversendes tilsynsobjektet sammen med eventuelle vedtak om pålegg. Sektortilsyn med tilsynsansvar skal sende kopier av tilsynsrapporter til NSM og bør også underrette sektordepartementet om resultatet av tilsynet.

Tilsynsrapporter og underrettelser må sendes innen rimelig tid og slik at departementet kan utøve sitt sektoransvar, og NSM sitt sektorovergripende ansvar, for forebyggende sikkerhetsarbeid.

4.5. Opplysninger fra tilsyn

Sikkerhetsloven har bestemmelser om håndtering av opplysninger fra tilsyn i:

> *§ 3-3. Generelle prinsipper for tilsyn (andre ledd)*
>
> *Opplysninger som tilsynsmyndigheten innhenter, kan bare brukes i forbindelse med tilsynet og i det forebyggende sikkerhetsarbeidet.*

Sikkerhetsloven har i tillegg bestemmelser om behandling av personopplysninger fremkommet i forbindelse med tilsyn:

> *§ 3-5. Tilsynsmyndighetens behandling av personopplysninger*
>
> *Tilsynsmyndigheten kan behandle personopplysninger dersom det er nødvendig for å utføre sine oppgaver.*
>
> *Behandlingen av personopplysninger må ikke utgjøre et uforholdsmessig inngrep i personvernet.*
>
> *Personopplysninger skal om mulig behandles ved hjelp av virksomhetens informasjonssystem, uten at de blir kopiert eller overført til tilsynsmyndigheten. Tilsynsmyndigheten kan likevel kreve kopi av personopplysninger når dette er nødvendig for å dokumentere om bestemmelser i loven er brutt.*
>
> *Kongen kan gi forskrift om tilsynsmyndighetens behandling av personopplysninger.*

Kravet om at opplysninger fra tilsyn kun skal benyttes i forbindelse med forebyggende sikkerhetsarbeid må forstås slik at opplysningene kan benyttes av:

- *virksomhetene* – som grunnlag for sitt forbedringsarbeid
- *sektordepartement* – for ivaretagelse av forebyggende sikkerhetsarbeid i egen sektor
- *tilsynsmyndigheter* – som grunnlag for det forebyggende sikkerhetsarbeidet
- *NSM* – for oppfølgning og for å etablere oversikt *over forebyggende sikkerhetsarbeid i virksomhet, sektor og landet som helhet*

Som ledd i tilsynsvirksomheten vil tilsynsmyndigheten få tilgang til personopplysninger. Behandling av slike opplysninger skal kun skje der dette, etter en konkret vurdering, fremstår som nødvendig og proporsjonalt med inngrepet behandlingen representerer.

Som hovedregel skal personopplysninger kun behandles ved hjelp av virksomhetens egne informasjonssystemer. Tilsynsmyndigheten kan kun kreve kopi av personopplysninger i den utstrekning dette er nødvendig for å påvise eller avkrefte lovbrudd. Dersom det tas slik kopi av personopplysninger, plikter tilsynsmyndigheten å varsle virksomheten at dette er gjort.

Bestemmelsene skal motvirke unødig spredning av personopplysninger, både av hensyn til grunnleggende sikkerhetsinteresser, den enkeltes personvern og tilliten til tilsynsmyndigheten.

4.6. NSMs tilsynsmetodikk

NSMs tilsyn er risikobaserte og gjennomføres som systemrevisjoner understøttet av fagspesifikke undersøkelser. Det vil si at tilsynene gjennomføres for å undersøke styringssystemet for sikkerhet samtidig som det gjennomføres undersøkelser innen de forskjellige sikkerhetsfagene som informasjonssikkerhet, informasjonssystemsikkerhet, objekt- og infrastruktursikkerhet og personellsikkerhet.

Systemrevisjonen gjennomføres med grunnlag i standarden NS-EN ISO 19011, herunder med prinsippene for revisjon:

- *integritet* – som grunnlag for profesjonell adferd
- *rettferdig presentasjon* – forpliktelse til å rapportere sannferdig og nøyaktig
- *nødvendig faglig omtanke* – anvendelsen av grundighet og dømmekraft ved revisjon
- *konfidensialitet* – sikring av informasjon
- *uavhengighet* – grunnlaget for upartiskhet ved revisjonen og saklighet på revisjonskonklusjonene
- *bevisbasert fremgangsmåte* – den fornuftige metoden for å komme frem til pålitelige og reproduserbare revisjonskonklusjoner i en systematisk revisjonsprosess.

Tilsyn gjennomføres normalt i form av stedlig tilsyn, men også andre tilsynsformer benyttes. Eksempler er dokumentundersøkelser (undersøkelser av innsendt dokumentasjon), tematilsyn (undersøkelser av avgrensede tilsyn ofte hos flere tilsynsobjekter) og tilsynssaker (i forbindelse med uønskede hendelser).

5. Reaksjoner etter tilsyn

Tilsynsmyndigheten kan sanksjonere brudd på sikkerhetslov og tilhørende forskrifter med ulike virkemidler som *pålegg, tvangsmulkt, overtredelsesgebyr* eller *politianmeldelse*. Tilsynsmyndigheten skal iht. sikkerhetsloven § 3-2 informere NSM om bruk av sanksjoner og slik bidra til enhetlig bruk av sanksjoner på tvers av sektorer.

5.1. Pålegg

Sikkerhetsloven har bestemmelser om pålegg etter tilsyn i:

§ 3-6. Pålegg (første ledd)

Tilsynsmyndigheten kan gi virksomheter pålegg om gjennomføring av tiltak som er nødvendige for å ivareta lovens formål. Pålegg om konkrete tiltak kan bare gis dersom kostnadene som påføres virksomheten, framstår som rimelige sett i forhold til det som kan oppnås ved tiltaket.

Påleggskompetanse etter sikkerhetsloven er lagt til sikkerhetsmyndigheten og sektormyndighet med tilsynsansvar. Pålegg vil som hovedregel omfatte krav om korrigering av avvik. I enkelt tilfeller kan det også være aktuelt å pålegge konkrete tiltak.

I de tilfellene hvor det pålegges konkrete tiltak, må disse være nødvendige for å ivareta lovens formål, og kostnadene forbundet med pålegget må være rimelige sett i forhold til det som kan oppnås ved tiltakene. Det må foretas en konkret vurdering av om tiltakene er uforholdsmessig kostbare sett i forhold til hva som er en akseptabel restrisiko for virksomheten.

Det understrekes at en kost/nytte-vurdering ikke kan resultere i at kravet til forsvarlig sikkerhet ikke oppfylles. Kravet om forsvarlig sikkerhetsnivå er absolutt og kan ikke avveies mot kostnader eventuelle tiltak vil medføre.

Pålegg gis som enkeltvedtak med de plikter og rettigheter som følger av forvaltningsloven, blant annet reglene om begrunnelse og klage.

5.2. Tvangsmulkt

Sikkerhetsloven har bestemmelser om tvangsmulkt i:

§ 11-2. Tvangsmulkt

Ved overtredelse av bestemmelser gitt i eller i medhold av §§ 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, § 9-2 første ledd, § 9-4 første ledd første punktum eller § 9-4 andre ledd første eller andre punktum, kan tilsynsmyndigheten fastsette en tvangsmulkt som løper inntil forholdet er brakt i orden. Det samme gjelder for pålegg gitt i medhold av § 3-6.

Et vedtak om tvangsmulkt kan påklages til departementet.

Et vedtak etter første ledd er særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Kongen kan gi forskrift om tvangsmulkt.

Bestemmelsene er utdypet i virksomhetsikkerhetsforskriften:

§ 92. Tvangsmulkt

En tvangsmulkt fastsatt med hjemmel i sikkerhetsloven § 11-2 kan fastsettes som en engangsmulkt eller løpende for hver dag, uke eller måned etter at fristen for å rette forholdet er gått ut. Tilsynsmyndigheten kan frafalle en påløpt tvangsmulkt.

Tilsynsmyndigheten kan ilegge en virksomhet som har overtrådt loven, løpende mulkt for å tvinge virksomheten til å rette opp i forholdet. Formålet med tvangsmiddelet er å få virksomheten til å handle i tråd med sikkerhetsloven. Mulkten må ikke være mer tyngende enn det som er nødvendig for å oppnå dette, og må dessuten være et egnet virkemiddel til å oppnå formålet.

Tvangsmulkt forutsetter at det er truffet gyldig enkeltvedtak som pålegger virksomheten å endre sin praksis, jf. § 3-6, og kan bare ilegges dersom pålegget er rettskraftig og fristen for å rette forholdet er gått ut.

5.3. Overtredelsesgebyr

Sikkerhetsloven har bestemmelser om overtredelsesgebyr i:

§ 11-3. Overtredelsesgebyr

Tilsynsmyndigheten kan pålegge en virksomhet overtredelsesgebyr dersom virksomheten eller noen som handler på dennes vegne, forsettlig eller uaktsomt

a) overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-3, 4-4, 4-5, 5-2, 6-2, 6-3, 7-3, 9-2 første ledd, 9-4 første ledd første punktum eller § 9-4 andre ledd første eller andre punktum

b) overtrer et pålegg gitt med hjemmel i § 3-6

c) gir uriktige eller ufullstendige opplysninger til tilsynsmyndigheten etter §§ 3-4 eller 4-5

d) medvirker til overtredelser som nevnt i bokstav a til c.

Ved fastsettelse av overtredelsesgebyrets størrelse skal det særlig legges vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning. Et vedtak om overtredelsesgebyr er et særlig tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13.

Adgangen til å pålegge overtredelsesgebyr foreldes etter fem år. Fristen avbrytes når tilsynsmyndigheten meddeler virksomheten at denne er mistenkt for overtredelse av loven eller vedtak fastsatt med hjemmel i loven.

Et vedtak om overtredelsesgebyr kan påklages til departementet.

Kongen kan gi forskrift om overtredelsesgebyr.

Overtredelsesgebyr kan ilegges ved forsettlig eller uaktsom overtredelse av bestemmelsene angitt i bokstav a til c.

Bestemmelsens andre ledd angir relevante momenter som skal tas i betraktning ved fastsettelsen av gebyrets størrelse. Momentene er relevante også ved vurderingen av **om** gebyr skal ilegges.

Virksomhetens ansvar strekker seg ut over egen organisasjon og omfatter også de som *handler på dennes vegne.* Dette betyr at det må være en viss tilknytning mellom virksomheten og den som har overtrådt bestemmelsen, eksempelvis leverandører eller underleverandører.

Ileggelse av overtredelsesgebyr er inngripende og må være forholdsmessig.

5.4. Politianmeldelse

§ 11-3. Straff

Den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av §§ 3-4, 4-3 eller § 5-2, § 5-3 første ledd, §§ 6-2, 6-3, 7-3, § 9-2 første ledd, § 9-4 første ledd første punktum eller § 9-4 andre ledd første eller andre punktum, eller overtrer et pålegg gitt av tilsynsmyndigheten i medhold av § 3-6, straffes med bot eller fengsel inntil 6 måneder eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som forsettlig eller grovt uaktsomt bryter taushetsplikt etter § 5-4 andre ledd eller § 6-6 femte ledd, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Den som overtrer et forbud fastsatt med hjemmel i § 7-5, straffes med bot eller fengsel inntil 1 år eller begge deler, hvis ikke forholdet går inn under en strengere straffebestemmelse.

Forsøk på overtredelser som nevnt i første til tredje ledd straffes på samme måte.

Tilsynsmyndighetene skal vurdere anmeldelse til Politiets sikkerhetstjeneste (PST) ved mistanke om brudd på bestemmelsene angitt i lovens § 11-3. Vurderingen skal omfatte overtredelsens alvorlighet og hvorvidt den skyldes uaktsomhet eller forsett.

6. Vedlegg A – Kriterier for forsvarlig sikkerhetsnivå

Vedlegget beskriver kort fremgangsmåte for vurdering av sikkerhetsnivå med hovedvekt på kriterier (i pkt. 6.3) for slik vurdering. Mer utfyllende veiledning i fremgangsmåten fremgår av NSMs øvrige veiledere, bla. *Veileder i sikkerhetsstyring* og i *Veileder for sikkerhetsgodkjenning av informasjonssystem.*

Virksomheten skal etablere de sikkerhetstiltak og -prosedyrer som er nødvendig for å oppnå forsvarlig sikkerhetsnivå for de skjermingsverdige verdiene. Dette fremkommer i sikkerhetsloven:

> *§ 4-3. Plikt til å gjennomføre sikkerhetstiltak og øvelser (første ledd, første setning)*
>
> *Virksomheten skal gjennomføre de forebyggende sikkerhetstiltak som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knytte til sikkerhetstruende virksomhet.*

Forsvarlig sikkerhetsnivå er oppnådd når risiko overfor de skjermingsverdige verdiene er håndtert til akseptabelt nivå.

Etterlevelse av NSMs konkrete sikkerhetsfaglige anbefalinger, eksempelvis gitt i tekniske veiledninger eller håndbøker, vil som hovedregel gi grunnlag for forsvarlig sikkerhetsnivå. Forutsetningen er at anbefalingene benyttes for forholdene de er utformet for og i samsvar med de rammer og forutsetninger som er lagt til grunn. Vurdering av forsvarlig sikkerhetsnivå blir da samsvarsvurdering med de aktuelle anbefalingene.

For forhold der NSM ikke har gitt anbefalinger eller der virksomheten ønsker annen risikohåndtering enn den NSM anbefaler, kan forsvarlig sikkerhetsnivå vurderes ved å undersøke hvorvidt etablerte (eller foreslåtte) sikkerhetstiltak er tilstrekkelige og hensiktsmessige.

6.1. Scenarioer[4]

Sikkerhetstiltakenes tilstrekkelighet og hensiktsmessighet undersøkes i forhold til aktuelle scenarioer overfor de skjermingsverdige verdiene. Scenarioene beskrives som relevante uønskede hendelser som kan påvirke:

- *fysiske forhold* – urettmessig (uautorisert) adgang til skjermingsverdige verdier, eksempelvis gjennom adgang til fysisk arkiv uten tjenstlig behov
- *elektroniske forhold* – inntrengning gjennom elektroniske grensesnitt eller elektromagnetisk avlesning eller påvirkning, eksempelvis gjennom datainntrengning
- *menneskelige forhold* – påvirkning av personell i roller med betydning for sikkerhet, eksempelvis gjennom sosial manipulering

[4] Veiledere og håndbøker innenfor respektive fagområder inneholder eksempler på scenarier for ulike tiltaksvurderinger.

- *organisatoriske forhold* – utnyttelse av svakheter i sikkerhetsorganisering, eksempelvis mangelfulle rutiner for varsling av uønskede hendelser

6.2. Aktører

Scenarioene konkretiseres ytterligere ved å angi mulige aktører bak hendelsene beskrevet ved:

6.2.1. Tilhørighet

- *eget personell*[5] *med tilgang* – dvs. medarbeidere i arbeidsforhold og som oppfyller ev. vilkår for tilgang i form av sikkerhetsklarering, autorisasjon og tjenstlige behov
- *eget personell uten tilgang*[3] – dvs. medarbeidere i arbeidsforhold
- *eksternt personell* – som ikke har tilknytting til virksomheten

6.2.2. Kapasitet (eller evne)

- *liten* – grunnleggende kompetanse, kjennskap til funksjon og operativt miljø fra åpne kilder, allment tilgjengelige ressurser
- *middels* – utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø, tilpassede ressurser
- *god* – tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø, nødvendige ressurser

6.2.3. Intensjon (eller vilje)

- *ubevisst,* uønsket handling
- *bevisst,* opportunistisk handling
- handling *med hensikt* og plan

6.3. Tiltaksvurdering

Sikkerhetstiltakenes tilstrekkelighet og hensiktsmessighet vurderes:

- for hvert av scenarioene det må beskyttes mot

[5] *eget personell* omfatter også innleide og personell hos leverandører når forhold med betydning for sikkerhet er regulert i avtale tilsvarende som for medarbeidere i arbeidsforhold

- i forhold til sikkerhetsgradering for berørt informasjon/klassifisering av berørt informasjonssystem, objekt eller infrastruktur

Hvorvidt allerede etablerte eller foreslåtte sikkerhetstiltak vil gi akseptabelt risikonivå og derigjennom forsvarlig sikkerhetsnivå vurderes i henhold til sammenstillingen i 6.3.1 og 6.3.2.

6.3.1. Vurdering av tiltak for å beskytte skjermingsverdig informasjon[6]

	EGET PERSONELL MED TILGANG	EGET PERSONELL UTEN TILGANG	EKSTERNE
BEGRENSET	**liten kapasitet** *eller* **ubevisst**	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**
KONFIDENSIELT	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**
HEMMELIG	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**
STRENGT HEMMELIG	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**

Leseveiledning:

BEGRENSET

Informasjonssystemet skal være sikret slik at eget personell (med eller uten tilgang) ikke kan forårsake uønskede hendelser overfor skjermingsverdig informasjon sikkerhetsgradert BEGRENSET når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eksterne skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistiskhandling.

KONFIDENSIELT

Informasjonen skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser overfor informasjon sikkerhetsgradert KONFIDENSIELT når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eget personell (uten tilgang) skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

[6] Skjermingsverdig informasjon som ikke er sikkerhetsgradert, det vil si som må beskyttes av andre hensyn en konfidensialitet, vurderes i forhold til klassifiseringen for informasjonssystem, objekt eller infrastruktur som berøres dersom informasjonen går tapt, blir endret eller blir utilgjengelig

Eksterne skal ikke kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

HEMMELIG

Informasjonen skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser overfor informasjon sikkerhetsgradert HEMMELIG selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser– ved bevisst opportunistisk handling.

Verken eget personell (uten tilgang) eller eksterne skal kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

STRENGT HEMMELIG

Det skal ikke være mulig å forårsake uønskede hendelser overfor informasjon sikkerhetsgradert STRENGT HEMMELIG selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – og selv om det foreligger hensikt og plan.

6.3.2. Vurdering tiltak for å beskytte skjermingsverdig objekt eller infrastruktur[7]

	EGET PERSONELL MED TILGANG	EGET PERSONELL UTEN TILGANG	EKSTERNE	FREKVENS[8]
UNDERSTØTTER	**liten kapasitet** *eller* **ubevisst**	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**	**høy – oftere enn 2 ganger/år**
VIKTIG	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**	**moderat – 1 gang/år**
KRITISK	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**	**lav – 1 gang/10år**
MEGET KRITISK	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**	**ubetydelig – sjeldnere enn 1 gang/ 10år**

[7] Sammenstillingen benyttes for vurdering av klassifisert objekt og infrastruktur. Den benyttes også for vurdering av informasjonssystem som ikke selv er klassifisert (som objekt) men som har avgjørende betydning for klassifisert objekt eller infrastruktur, og sammenstillingen benyttes for vurdering av skjermingsverdig informasjon som ikke er sikkerhetsgradert, det vil si som må beskyttes av andre hensyn en konfidensialitet. Vurderingen gjennomføres da i forhold til klassifiseringen for objekter eller infrastruktur som berøres dersom informasjon går tapt, blir endret eller blir utilgjengelig.

Med *understøtter* menes informasjonssystem som ikke er skjermingsverdig, det vil si som ikke har avgjørende betydning for klassifisert objekt (og heller ikke selv er klassifisert), men som likevel har betydning for slike. Sikkerhetslovens krav om forsvarlig sikkerhetsnivå skal forstås slik at også slike systemer må sikres i nødvendig grad. Det er imidlertid ikke krav om godkjenning av disse informasjonssystemene.

[8] Sannsynlighet for bortfall

Leseveiledning:

UNDERSTØTTER

Informasjonssystemet skal være sikret slik at ikke eget personell (med eller uten tilgang) kan forårsake uønskede hendelser som påvirker funksjon i informasjonssystem som UNDERSTØTTER skjermingsverdig objekt, eller infrastruktur, når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eksterne skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

VIKTIG

Objektet eller infrastrukturen skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser som påvirker funksjon i objekt eller infrastruktur klassifisert VIKTIG når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eget personell (uten tilgang) skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

Eksterne skal ikke kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

KRITISK

Objektet eller infrastrukturen skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser som påvirker funksjon objekt eller infrastruktur klassifisert KRITISK selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

Eget personell (uten tilgang) eller eksterne skal ikke kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

MEGET KRITISK

Det skal ikke være mulig å forårsake uønskede hendelser overfor objekt eller infrastruktur klassifisert MEGET KRITISK selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – og selv om det foreligger hensikt og plan.

7. Vedlegg B – Kriterier for sikkerhetsstyring

Vedlegget beskriver kort krav om sikkerhetsstyring med hovedvekt på *kriterier* for vurdering av samsvar med disse kravene. Mer utfyllende veiledning i krav om sikkerhetsstyring fremgår av NSMs *Veileder i sikkerhetsstyring*.

Forebyggende sikkerhetsarbeid omfatter alle aktiviteter med betydning for beskyttelsen av skjermingsverdige verdier. Forebyggende sikkerhetsarbeid skal utføres innenfor rammene av et styringssystem for sikkerhet etter sikkerhetsloven:

> *§ 4-1. Sikkerhetsstyring (første ledd andre setning)*
>
> *Forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem.*

Kravet om sikkerhetsstyring er utdypet i virksomhetsikkerhetsforskriften kapittel 2:

> *§ 3. Styringssystem for sikkerhet*
>
> *En virksomhet som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.*

Sikkerhetsstyringssystemet skal omfatte hele det forebyggende sikkerhetsarbeidet, dvs. både aktiviteter dedikert for sikkerhet og aktiviteter som kan ha betydning for sikkerhet. Dette innebærer at styringssystemet for sikkerhet skal omfatte grunnprinsippene i sikkerhetsstyring:

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

Styringssystemet for sikkerhet skal integreres i virksomhetsstyringen for øvrig. Eksempelvis kan virksomhetens kompetansestyring utvides til også å omfatte kompetanse innen beskyttelse av skjermingsverdige verdier. Ved samordning er det viktig å være oppmerksom på at forebyggende sikkerhetsarbeid vil medføre behandling av skjermingsverdig informasjon. Samordningen må derfor ivareta behovet for beskyttelse av slik informasjon mot uautorisert tilgang.

Styringssystemet for sikkerhet kan etableres og samordnes gjennom tilpassing av eksisterende styringssystem, og/eller med utgangspunkt i anerkjente standarder for styring som ISO 9000-serien og ISO 27000-serien. Forutsetningen er da at (det tilpassede) styringssystemet:

- dekker hele det forebyggende sikkerhetsarbeidet, dvs. omfatter alle styringselementene
- er dimensjonert i forhold til risiko for sikkerhetstruende virksomhet

- oppfyller kravene i og i medhold av sikkerhetsloven, jf. påfølgende beskrivelse av styringselementene.

7.1. Sikkerhetsledelse

Virksomhetens leder har det endelige ansvaret for det forebyggende sikkerhetsarbeidet i virksomheten og utført av andre for virksomheten og for at dette arbeidet gir forsvarlig sikkerhet som resultat etter sikkerhetsloven:

§ 4-1. Sikkerhetsstyring (første ledd første setning)
Virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet.

Kravet er utdypet gjennom krav om styringsdokument i virksomhetsikkerhetsforskriften:

§ 4. Styringsdokument for det forebyggende sikkerhetsarbeidet
Lederen for en virksomhet skal fastsette et styringsdokument som beskriver
a) hvilke deler av sikkerhetsloven med forskrifter som gjelder for virksomheten
b) roller og ansvar i virksomhetens forebyggende sikkerhetsarbeid, jf. § 6
c) prinsipper for virksomhetens sikkerhetsarbeid.
Styringsdokumentet skal gjøres kjent og være tilgjengelig for virksomhetens ansatte og for leverandører og andre eksterne samarbeidspartnere, i den grad det er nødvendig for å oppfylle virksomhetens plikter etter sikkerhetsloven.

Sikkerhetsledelse skal utøves gjennom overordnede føringer om:

- *verdier som må beskyttes* – eksempelvis skjermingsverdig informasjon med tilhørende sikkerhetsgradering og/eller skjermingsverdig objekt eller infrastruktur med tilhørende klassifisering
- *fordeling av ansvar og myndighet* – for alle aktiviteter med betydning for sikkerhet
- *prinsipper* – eksempelvis gjennom henvisning til standarder og metoder for sikkerhetsstyring og risikostyring

… kort beskrevet i virksomhetens styringsdokument for forebyggende sikkerhet gjennom informasjon om forpliktelser og forventning til forebyggende sikkerhetsarbeid, fra virksomhetens ledelse til alt personell som utfører aktiviteter med betydning for sikkerhet.

7.1.1. Ressurser og kompetanse

Virksomhetsikkerhetsforskriften krever at det stilles nødvendige ressurser til rådighet for forebyggende sikkerhetsarbeid i:

§ 7. Ressurser og kompetanse (første ledd)
En virksomhet skal forvalte og utvikle det forebyggende sikkerhetsarbeidet sitt på en forsvarlig måte.

Sikkerhetsledelse skal utøves også gjennom tilrettelegging for forebyggende sikkerhetsarbeid ved å stille nødvendige økonomiske ressurser, tilstrekkelig tid og hensiktsmessige verktøy til rådighet for arbeidet.

7.2. Sikkerhetsorganisering

Ansvar og myndighet, plikter og rettigheter knyttet til aktiviteter med betydning for beskyttelse av skjermingsverdige verdier, må fordeles og kommuniseres, og personellet må settes i stand til å utføre det forebyggende sikkerhetsarbeidet som forutsatt i sikkerhetsloven:

§ 4-1. Sikkerhetsstyring (andre ledd første punktum)

Virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse.

Kravet er videre utdypet gjennom krav til informasjon og kompetanse i virksomhetsikkerhetsforskriften:

§ 7. Ressurser og kompetanse (andre ledd)

Virksomheten skal utføre følgende tiltak overfor de som kan få tilgang til skjermingsverdige verdier gjennom å utføre arbeid eller tjenester for virksomheten:

a) få bekreftet identiteten deres med gyldig legitimasjon

b) sørge for at de kjenner til de relevante delene av styringssystemet for sikkerhet

c) sørge for tilstrekkelig kompetanse om sikkerhet

d) informere om endringer i kravene til sikkerheten

e) klarlegge at personene kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser.

Alle som utfører aktiviteter med betydning for sikkerhet skal kjenne de grunnleggende forutsetningen for egen arbeidsutførelse. Dette omfatter nødvendig informasjon om risiko for sikkerhetstruende virksomhet og nødvendig kjennskap til sikkerhetsstyringssystemet.

Den enkelte skal være kjent med eget ansvar, egen myndighet og hvordan aktivitetene skal utføres. Slik informasjon kan eksempelvis gis gjennom rollebeskrivelser.

Den enkelte skal ha riktig kompetanse til å utføre aktiviteter sikkert og som besluttet. Riktig kompetanse oppnås og opprettholdes gjennom planmessig opplæring, kvalifisering og kompetansevedlikehold.

7.2.1. Roller i det forebyggende sikkerhetsarbeidet

Virksomhetsikkerhetsforskriften har krav om fordeling av ansvar og myndighet for roller i det forebyggende sikkerhetsarbeidet i:

§ 6. Roller i og ansvar for det forebyggende sikkerhetsarbeidet (første og tredje ledd)

Lederen for en virksomhet skal fordele roller i og ansvar for det forebyggende sikkerhetsarbeidet, slik at kravene gitt i eller med hjemmel i sikkerhetsloven ivaretas. Rollene og ansvarsfordelingen skal gjøres kjent i virksomheten.

Kontrollen av styringssystemet for sikkerhet skal om mulig utføres av andre enn de som har styrende eller utøvende oppgaver i det forebyggende sikkerhetsarbeidet.

Forebyggende sikkerhetsarbeid organiseres med utgangspunkt i at virksomhetens ledelse beslutter overordnede føringer, linjeledere har ansvar for sikkerhetsarbeidet innen eget myndighetsområde og personellet har ansvar for at egen arbeidsutførelse er sikker og som besluttet.

Utførelse og oppfølging av aktiviteter med betydning for sikkerhet skal om mulig skje uavhengig av hverandre, blant annet for å sikre at medarbeidere ikke settes til å kontrollere egen arbeidsutførelse.

Virksomheten kan utpeke roller for utførelse av aktiviteter dedikert for sikkerhet. Antall og typer av roller avhenger av virksomhetens formål og kompleksitet og den risiko skjermingsverdige verdier er utsatt for. Som minimum er det aktuelt å fordele ansvar og myndighet for å følge opp og bistå det forebyggende sikkerhetsarbeidet til en rolle som sikkerhetsleder.

7.2.2. Taushetsplikt

Sikkerhetsloven har krav om taushetsplikt i:

§ 5-4. Tilgang til og taushetsplikt med hensyn til sikkerhetsgradert informasjon

Sikkerhetsgradert informasjon skal bare overlates til personer som har tjenstlig behov og er autorisert for tilgang til slik informasjon.

Alle som får tilgang til sikkerhetsgradert informasjon som ledd i arbeidet eller tjenesten for en virksomhet som omfattes av loven, har taushetsplikt om innholdet. Taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet.

Alle som utfører aktiviteter med betydning for sikkerhet har taushetsplikt, også etter at arbeidsforholdet er avsluttet.

Taushetsplikten skal være kjent for dem den gjelder gjennom informasjon om pliktens omfang, varighet og konsekvenser dersom den brytes.

Taushetsplikten skal erkjennes gjennom taushetserklæringer som oppbevares av virksomheten.

7.2.3. Sikkerhet ved fratredelse

Virksomhetsikkerhetsforskriften har krav om sikkerhet når personell fratrer, eller skifter stilling eller funksjon i:

§ 7. Ressurser og kompetanse (tredje ledd)

Når et arbeidsforhold eller en tjeneste avsluttes, skal virksomheten sikre at den som slutter, ikke lenger har tilgang til skjermingsverdige verdier. Den som slutter, skal informeres om at taushetsplikten etter sikkerhetsloven § 5-4 andre ledd fremdeles gjelder.

Tilgang til skjermingsverdige verdier skal endres når tjenstlig behov endres, eksempelvis som følge av endringer i arbeidsforholdet. Det innebærer blant annet at virksomheten må sørge for at medarbeidere som fratrer ikke lenger har tilgang til verdiene.

7.3. Sikkerhetstiltak og -prosedyrer

Virksomheten skal etablere de sikkerhetstiltak og -prosedyrer som er nødvendig for å oppnå forsvarlig sikkerhetsnivå etter sikkerhetsloven.

Sikkerhetsloven har krav om sikkerhetstiltak i:

§ 4-3. Plikt til å gjennomføre sikkerhetstiltak og øvelser (første ledd og andre ledd)

Virksomheten skal gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet. Slike tiltak kan gjennomføres i sammenheng med andre forebyggende sikkerhetstiltak i virksomheten, så lenge kravene i denne loven oppfylles.

Kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket.

Kravet er utdypet gjennom krav til sikkerhetstiltak i virksomhetsikkerhetsforskriften:

§ 14. Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenoppretting (første og andre ledd)

Grunnsikringstiltak skal bidra til et forsvarlig sikkerhetsnivå i virksomheter i en normaltilstand. Grunnsikringstiltakene kan være

a) fysiske, elektroniske, menneskelige eller organisatoriske barrierer

b) systemer som skal oppdage og varsle om aktiviteter eller hendelser

c) systemer og rutiner for å avklare aktiviteter og hendelser og bakgrunnen for dem

d) oppfølging av uønskede aktiviteter og uønskede hendelser

e) en kombinasjon av tiltakene nevnt i bokstav a til d.

En virksomhet skal, i god tid før en skjermingsverdig verdi etableres, fastsette hvilke grunnsikringstiltak som skal beskytte den. Virksomheten skal også vurdere om det er behov for slike tiltak i forbindelse med avviklingen av den skjermingsverdien verdien.

Sikkerhetstiltak skal etableres med grunnlag i risikovurdering og slik at risiko for sikkerhetstruende virksomhet reduseres til akseptabelt nivå slik at forsvarlig sikkerhetsnivå oppnås.

Grunnsikring etableres som balansert sikring i form av barrierer, deteksjon, verifikasjon og/eller reaksjon i sammenheng og med tanke på risiko for sikkerhetstruende virksomhet i normaltilstanden.

Virksomheten velger selv mest hensiktsmessige og kostnadsoptimale kombinasjon av tiltak og kan ikke pålegges etablering av urimelig kostbare tiltak. Kravet om forsvarlig sikkerhetsnivå er imidlertid absolutt og virksomheten kan ikke unnlate etablering av de tiltak som er nødvendig for å oppnå dette nivået med henvisninger til kostnader.

7.3.1. Beredskap

Virksomhetsikkerhetsforskriften har krav om beredskap i:

§ 14. Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenopprettelse (tredje, fjerde og femte ledd)

En virksomhet skal planlegge påbyggingstiltak som kan iverksettes dersom økt risiko medfører at det ikke er tilstrekkelig med grunnsikringstiltakene. Påbyggingstiltakene skal kunne iverksettes i løpet av kort tid, og de skal kunne avvikles dersom risikoen reduseres i tilstrekkelig grad.

Dersom den økte risikoen vedvarer, skal virksomheten vurdere om påbygningstiltakene skal bli en del av grunnsikringen. I slike tilfeller skal virksomheten planlegge nye påbyggingstiltak.

Virksomheten skal planlegge skadebegrensningstiltak som kan iverksettes i situasjoner som ikke kan håndteres fullt ut med grunnsikrings- og påbyggingstiltakene.

Tiltak for påbygging, gjenoppretting og skadebegrensning skal forberedes som beredskap i tilfelle risikoen for sikkerhetstruende virksomhet øker i forhold til normaltilstanden. Som for grunnsikringstiltakene skal beredskapstiltakene skal etableres som tiltak og prosedyrer i sammenheng.

Når påbygningstiltak har vært etablert over tid overfor en vedvarende forhøyet risiko, skal det vurderes å forsterke grunnsikringen. I så fall må nye påbygningstiltak forberedes for ytterligere økt risiko.

7.3.2. Prinsipper for valg av sikkerhetstiltak - og prosedyrer

Virksomhetsikkerhetsforskriften har krav om prinsipper for valg og utforming av sikkerhetstiltak i:

§ 15. Prinsipper ved valg og utforming av sikkerhetstiltak (første og andre ledd)

Når en virksomhet velger ut og utformer sikkerhetstiltak, skal følgende prinsipper legges til grunn:

a) Sikkerhetstiltakene skal ikke ha annen funksjonalitet eller større kompleksitet enn nødvendig.

b) Det skal ikke gis en mer omfattende tilgang til skjermingsverdige verdier enn nødvendig.

c) Svikt i et enkelt tiltak skal ikke kunne føre til kompromittering av skjermingsverdige verdier.

d) Sikkerhetstiltak skal i minst mulig grad være avhengige av hverandre, og flere sikkerhetstiltak skal dermed ikke kunne svekkes eller settes ut av funksjon samtidig, for eksempel som følge av én enkelt feil eller hendelse.

e) Effekten av sikkerhetstiltakene skal være tilnærmet lik for alle skjermingsverdige verdier med samme sikkerhetsbehov.

Sikkerhetstiltakene skal være samordnet. Kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket.

Prinsippene om minimalisme, minste privilegium, sikring i dybden, motstandsdyktighet og balansert styrke skal vurderes ved valg av sikkerhetstiltak. Sikkerhetstiltak skal fungere i sammenheng slik at de ikke motvirker hverandre eller dupliseres unødvendig.

7.4. Forholdet til andre virksomheter

Andre virksomheters forebyggende sikkerhetsarbeid kan påvirke sikkerhetsnivået i virksomheten og virksomhetens sikkerhetsarbeid kan påvirke sikkerhetsnivået hos andre enn virksomheten selv. Risiko

for slik påvirkning må håndteres til akseptabelt nivå. Dette følger blant annet av sikkerhetslovens generelle krav om sikkerhetsstyring i § 4-1 utdypet blant annet i virksomhetsikkerhetsforskriften §§ 3 og 4.

Krav til forholdet med leverandører og oppdragsgivere fremkommer av sikkerhetsloven:

> *§ 4-1. Sikkerhetsstyring (annet ledd første setning)*
>
> *Virksomheten skal sørge for at ansatte, leverandører og oppdragstakere har tilstrekkelig risiko- og sikkerhetsforståelse.*

Kravet er utdypet gjennom krav til sikkerhet i anskaffelser i virksomhetsikkerhetsforskriften:

> *§ 18. Krav til sikkerhet i anskaffelser*
>
> *Dersom en anskaffelse kan gi leverandøren eller dennes personell en mulighet til å påvirke et skjermingsverdig informasjonssystem eller objekt eller en skjermingsverdig infrastruktur, skal oppdragsgiveren vurdere risikoen for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet, og hvordan risikoen skal håndteres. Dersom virksomheten kommer til at anskaffelsen vil medføre en ikke ubetydelig risiko, skal virksomheten varsle departementet etter sikkerhetsloven § 9-4.*
>
> *Dersom en anskaffelse gir tilgang til skjermingsverdige informasjonssystemer eller skjermingsverdig ugradert informasjon, skal det inngås en avtale mellom virksomheten og leverandøren, hvor det fastsettes hvordan leverandøren skal forholde seg til de kravene som gjelder for anskaffelsen.*

Forholdet til andre virksomheter skal omfattes av de risikovurderinger som ligger til grunn for det forebyggende sikkerhetsarbeidet.

Ansvar og myndighet for forebyggende sikkerhetsarbeid mellom virksomheten og andre virksomheter må være avklart og i nødvendig grad formalisert gjennom avtale som også omfatter vilkår om:

- nødvendig informering av personellet om risiko og sikkerhetsstyrings
- håndtering av uønskede hendelser

… virksomhetene i mellom

Anskaffelser som kan gi leverandør, eller dennes personell, mulighet for å påvirke skjermingsverdige verdier skal håndteres som sikkerhetsgradert anskaffelse, jf. virksomhetsikkerhetsforskriften kapittel 13.

7.5. Sikkerhetsoppfølging

Det forebyggende sikkerhetsarbeid skal kontinuerlig forbedres. Et viktig element i forbedringsprosessen er sikkerhetsoppfølging. Sikkerhetsloven har krav om sikkerhetsoppfølging i:

> *§ 4-1. Sikkerhetsstyring (første ledd siste setning)*
>
> *Sikkerhetstilstanden i virksomheten skal regelmessig kontrolleres.*

Sikkerhetstilstanden skal kontrolleres gjennom jevnlig evaluering (intern sikkerhetsrevisjon) og leders årlige periodisk evaluering (ledelsens gjennomgåelse). Også håndtering av uønskede hendelser er en

del av oppfølgingen i form av undersøkelser av hendelsenes underliggende årsaker og påfølgende korrigering for å hindre gjentagelse.

7.5.1. Håndtering av uønskede hendelser

Virksomhetsikkerhetsforskriften har krav om håndtering av uønskede hendelser i:

> *§ 8. Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon (første ledd)*
>
> *Ved sikkerhetstruende virksomhet eller avvik fra styringssystemet for sikkerhet skal en virksomhet gjennomføre umiddelbare tiltak for å redusere skadeomfanget og gjenopprette et forsvarlig sikkerhetsnivå. Det skal rapporteres om den sikkerhetstruende virksomheten eller avviket internt og til andre som kan bli berørt i stor grad. Virksomheten skal vurdere konsekvensene av den sikkerhetstruende virksomheten eller avviket.*

Uønskede hendelser som sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon skal håndteres for å begrense skade og hindre gjentagelse.

Håndtering av uønskede hendelser skal omfatte varsling, iverksetting av strakstiltak for å begrense skade, etablering av permanente korrigerende tiltak for å hindre gjentagelse samt evaluering av om de de korrigerende tiltakene fungerer som forutsatt.

Uønskede hendelser varsles til den som har ansvar og myndighet for håndtering av uønskede hendelser, inkl. for beslutning om etablering av permanente korrigerende tiltak. Virksomhetens leder skal varsles om saker som er viktige for det forebyggende sikkerhetsarbeidet.

7.5.2. Evaluering av forebyggende sikkerhetsarbeid

Virksomhetsikkerhetsforskriften har krav om evaluering av det forebyggende sikkerhetsarbeidet i:

> *§ 9. Evaluering og øvelser (første og tredje ledd)*
>
> *En virksomhet skal regelmessig evaluere om kravet til et forsvarlig sikkerhetsnivå er oppfylt og minst én gang i året evaluere om styringssystemet for sikkerhet er egnet til å sørge for at kravet oppfylles, jf. § 5.*
>
> *…*
>
> *Resultatet av evalueringer og øvelser skal inngå i den årlige gjennomgangen av det forebyggende sikkerhetsarbeidet i virksomheten.*

Evaluering av det forebyggende sikkerhetsarbeidet skal gjennomføres for å avklare om sikkerhetsstyringssystemet oppfyller kravene i sikkerhetsloven med forskrifter og er etablert som besluttet.

Evalueringen gjennomføres som periodisk undersøkelse og kan med fordel gjennomføres som intern sikkerhetsrevisjon (systemrevisjon). Avhengig av systemets omfang og kompleksitet kan revisjonen planlegges som en årlig undersøkelse av hele systemet, eller som del-undersøkelser slik at hele system undersøkes i løpet av et år.

Revisjonskriterier er krav i sikkerhetslovens med forskrifter og virksomhetens sikkerhetsstyringssystem.

Resultater fra revisjonen skal inngå som del av ledelsens gjennomgang av det forebyggende sikkerhetsarbeidet. Avvik fra revisjonskriteriene skal håndteres tilsvarende som for uønskede hendelser.

7.5.2.1. Øvelser

Sikkerhetsloven har krav om øvelser i:

> *§ 4-3. Plikt til å gjennomføre sikkerhetstiltak og øvelser (tredje ledd)*
>
> *Virksomheten skal regelmessig gjennomføre øvelser for å vurdere effekten av iverksatte sikkerhetstiltak.*

Kravet er utdypet i virksomhetsikkerhetsforskriften:

> *§ 9. Evaluering og øvelser (andre ledd)*
>
> *Virksomheten skal regelmessig gjennomføre øvelser for å kontrollere effekten av sikkerhetstiltakene i en normalsituasjon og av tiltakene som er planlagt ved økt trusselnivå. Er virksomheten avhengig av andre virksomheter for å fungere slik den skal, skal virksomheten be de andre virksomhetene om å delta på øvelser når det er relevant.*

Øvelser skal gjennomføres for å teste om etablerte sikkerhetstiltak fungerer etter intensjonen. Med bakgrunn i gjennomføring av øvelser skal virksomheten vurdere om det mangler sikkerhetstiltak eller om det er mangler ved etablerte sikkerhetstiltak. Virksomheten skal i tillegg gjennomføre øvelser som ledd i å utdanne og trene eget personell i situasjoner ved økt trusselnivå.

7.5.3. Leders gjennomgang av forebyggende sikkerhetsarbeid

Virksomhetsikkerhetsforskriften har krav om leders gjennomgang av det forebyggende sikkerhetsarbeidet i:

> *§ 10. Gjennomgang av det forebyggende sikkerhetsarbeidet av virksomhetens leder*
>
> *Lederen for en virksomhet skal årlig foreta en helhetlig gjennomgang av virksomhetens forebyggende sikkerhetsarbeid for å vurdere om styringssystemet for sikkerhet fungerer etter hensikten.*
>
> *Virksomheten skal gjennomføre nødvendige forbedringer i det forebyggende sikkerhetsarbeidet og i styringssystemet for sikkerhet.*

Leders gjennomgang av det forebyggende sikkerhetsarbeidet skal gjennomføres for å avklare om styringssystemet er hensiktsmessig eller om det er behov for tilpassinger som følge av endringer:

- i virksomheten – eksempelvis endringer i de skjermingsverdige verdiene
- eksternt for virksomheten – eksempelvis endringer i trusler overfor de skjermingsverdige verdiene

Ledelsens gjennomgang (ledelsens gjennomgåelse) er et årlig møte som ledes av virksomhetens leder og der alle øvrige ledere som påvirker eller kan påvirkes av sikkerhetsstyringssystemet, deltar.

Grunnlag for møtet er informasjon om siste års forebyggende sikkerhetsarbeid, blant annet fra håndtering av uønskede hendelser og fra revisjoner, samt informasjon om endringer (interne og eksterne) som kan påvirke det forebyggende sikkerhetsarbeidet. Ledelsens gjennomgåelse avsluttes med leders beslutning om (ev.) endringer i sikkerhetsstyringssystemet.

7.6. Sikkerhetsdokumentasjon

Sikkerhetsstyringssystemet skal dokumenteres – som grunnlag for å informere om hvordan det forebyggende sikkerhetsarbeidet skal utføres og som registrering av hvordan arbeidet er utført. Sikkerhetsloven har krav om sikkerhetsdokumentasjon i:

> *§ 4-4. Krav til dokumentasjon (første ledd)*
>
> *Virksomheten skal dokumentere vurderingen av risiko og de gjennomførte og planlagte sikkerhetstiltakene.*

Kravet er utdypet i virksomhetsikkerhetsforskriften:

> *§ 11. Dokumentasjon av styringssystem for sikkerhet*
>
> *Virksomheten skal dokumentere at styringssystemet for sikkerhet og sikkerhetstiltakene gir et forsvarlig sikkerhetsnivå, jf. § 5.*

Sikkerhetsstyringssystemet skal dokumenteres i det omfang det er nødvendig for å sikre at aktiviteter utføres sikkert og som besluttet, og slik at beslutninger og resultater av arbeidsutførelse kan gjenfinnes som grunnlag for (senere) håndtering av uønskede hendelser.

Sikkerhetsstyringssystemet skal dokumenteres gjennom:

- *styrende dokumenter* – som beskriver eksterne og interne (overordnede) føringer for det forebyggende sikkerhetsarbeidet, eksempelvis virksomhetens styringsdokument for forebyggende sikkerhetsarbeid, sikkerhetsmål og planer
- *utførende dokumenter* – som beskriver hvordan aktiviteter med betydning for sikkerhet utføres, eksempelvis prosedyrebeskrivelser, arbeidsinstrukser, handlingsplaner og sikkerhetstiltak
- *kontrollerende dokumenter* – som beskriver resultater fra gjennomføring av aktiviteter med betydning for sikkerhet, eksempelvis registreringer fra håndtering av uønskede hendelser og fra evaluering og referater fra ledelsens gjennomgåelse

Sikkerhetsdokumentasjonen skal være sporbar og kontrollert gjennom dokumentstyring som omfatter regler for merking, utarbeidelse, godkjenning, distribuering, oppbevaring, tilbaketrekking og avhending. Sikkerhetsdokumentasjon vil ofte inneholde skjermingsverdig informasjon og skal da beskyttes mot utilsiktet tilgang.

8. Vedlegg C – Kriterier for risikostyring

Vedlegget beskriver kort krav om risikostyring med hovedvekt på *kriterier* for vurdering av samsvar med disse kravene. Mer utfyllende veiledning i krav om risikostyring fremgår av NSMs *Veileder i sikkerhetsstyring*.

Risikostyring omfatter identifisering av risiko overfor virksomhetens skjermingsverdige verdier og håndtering av denne risikoen til akseptabelt nivå slik at forsvarlig sikkerhetsnivå oppnås.

8.1. Risikostyring

Risiko identifiseres gjennom risikovurderinger og sikkerhetsloven har krav om vurdering av risiko i:

§ 4-2. Vurdering av risiko (første til tredje ledd)

Virksomheten skal regelmessig gjennomføre vurdering av risiko. Vurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

Virksomheten skal som del av vurderingen kartlegge hvilke virksomheter den er avhengig av for å fungere som den skal.

Vurderingen skal gjennomgås jevnlig og om nødvendig revideres.

Kravet er utdypet i virksomhetsikkerhetsforskriften:

§ 12 . Vurdering av risiko

Når en virksomhet vurderer risiko, skal den ta hensyn til

a) hvilken betydning virksomhetens skjermingsverdige verdier har for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser

b) hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for

c) sannsynligheten for at sikkerhetstruende virksomhet kan inntreffe

d) hvilke sårbarheter som er knyttet til de skjermingsverdige verdiene

e) konsekvensen av sikkerhetstruende virksomhet for de skjermingsverdige verdiene

f) i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.

Behovet for å gjennomføre en ny helhetlig vurdering av risikoen skal vurderes årlig.

Dersom det planlegges, gjennomføres eller inntreffer endringer som kan påvirke skjermingsverdige verdier i vesentlig grad, skal virksomheten vurdere hvilken risiko endringene medfører.

Risikovurderinger skal gjennomføres som grunnlag for ny håndtering av skjermingsverdige verdier og deretter ved alle endringer som kan påvirke beskyttelsen av disse verdiene. Dette kan være endringer internt i virksomheten eller endringer eksternt for virksomheten.

Virksomheten bestemmer selv risikovurderingenes dekningsområde. Flere verdier og flere forhold kan dekkes av samme risikovurdering, eller vurderinger kan gjennomføres for avgrensede verdier og forhold. Sistnevnte fremgangsmåte er særlig aktuell ved interne eller eksterne endringer av begrenset omfang. *Forutsetningen er at det er gjennomført risikovurderinger med tilstrekkelig dekning og som er oppdaterte nok til å gi grunnlag for forebyggende sikkerhetsarbeid med forsvarlig sikkerhetsnivå som resultat*.

Risikovurderinger skal omfatte:

- *informasjon om skjermingsverdige verdier* – blant annet i form av opplysninger om sikkerhetsgradering og/eller klassifisering av disse verdiene hentet
- *avdekking av sårbarheter* – inkludert vurdering av konsekvens av at sikkerhetstruende virksomhet inntreffer
- *identifisering av trusler overfor skjermingsverdige verdier* – inkludert vurdering av sannsynlighet for at sikkerhetstruende virksomhet inntreffer

Informasjon om sikkerhetsgradering og/eller klassifisering av skjermingsverdige verdier skal fremgå av virksomhetens verdivurderinger og/eller skadevurderinger.

Avdekking av sårbarheter, identifisering av trusler, og vurderinger av sannsynlighet og konsekvens kan gjennomføres med utgangspunkt i scenarioer som beskriver relevante uønskede hendelser som kan påvirke fysiske, elektroniske, menneskelige og/eller organisatoriske forhold.

Scenarioene kan konkretiseres ytterligere ved å angi mulige aktører bak hendelsene, og dennes tilhørighet til virksomheten og kapasitet og intensjon til å forårsake hendelser.

Risikovurderinger kan med fordel gjennomføres i henhold til anerkjente standarder for risikovurdering eller -analyse som NS-5014, NS-583X-serien eller ISO-31000-serien.

8.2. Risikohåndtering

Virksomhetsikkerhetsforskriften har krav om risikohåndtering i:

> *§ 13. Håndtering av risiko*
>
> *Når en virksomhet skal håndtere en risiko, skal den vurdere*
>
> *a) om risikoen er akseptabel*
>
> *b) å endre sårbarheten til de skjermingsverdige verdiene ved grunnsikringstiltak og påbyggingstiltak*
>
> *c) hvordan virksomheten kan påvirke konsekvensene som kan inntreffe dersom de skjermingsverdige verdiene rammes, for eksempel ved å endre redundansen eller iverksette tiltak for skadebegrensning og gjenopprettelse*
>
> *d) å gjøre seg mindre avhengig av andre virksomheter*
>
> *e) å håndtere risikoen på andre måter.*

Virksomheten skal sende en oversikt over andre virksomheter den er avhengig av for å fungere som den skal, til Nasjonal sikkerhetsmyndighet og det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren.

Sikkerhetsstyringssystemet skal dimensjoneres i forhold til risiko overfor de skjermingsverdige verdiene. Dette innebærer at sikkerhetstiltak skal etableres med utgangspunkt i risikovurderinger.

Risiko kan håndteres ved å begrense sårbarheter eller konsekvenser av at sikkerhetstruende virksomhet inntreffer. Risikohåndtering gjennom etablering av sikkerhetstiltak og -prosedyrer er nærmere beskrevet i kapittel 7.3.

Forsvarlig sikkerhetsnivå er oppnådd når risiko er redusert til akseptabelt nivå. Dette innebærer at resultater fra risikovurderinger må sammenlignes med fastlagt nivå for akseptabel risiko for å avgjøre om risikohåndteringen er tilstrekkelig eller om ytterligere sikkerhetstiltak må til.

Nivå for akseptabel risiko avledes av forsvarlig sikkerhetsnivå og må være konkret nok til å fungere som sammenligningsgrunnlag for resultater fra risikovurderinger. Eksempler på slik konkretisering fremgår av tabellene i vedlegg 1. Vurderingskriteriene her kan benyttes som sammenligningsgrunnlag for resultater fra risikovurderinger gjennomført i henhold til metoden (tiltaksvurderingen) beskrevet i dette vedlegget.

8.3. Avhengigheter

I den grad virksomheten er avhengig av (eksterne) ressurser/andre virksomheter for å håndtere og beskytte skjermingsverdigeverdier, må også slike forhold dekkes av risikovurderinger.

Sikkerhetsloven har krav om beskyttelse mot sikkerhetstruende virksomhet, det vil si mot tilsiktede handlinger. Sikkerhetsloven har også krav om håndtering av avhengigheter og uønskede hendelser overfor disse er ikke avgrenset til slike handlinger. Risikovurderinger som dekker avhengigheter må derfor omfatte Scenarioer knyttet til utilsiktede hendelser.

I henhold til virksomhetsikkerhetsforskriften:

§ 13. Håndtering av risiko (første ledd bokstav d)

Når en virksomhet skal håndtere en risiko, skal den vurdere

…

d) å gjøre seg mindre avhengig av andre virksomheter

… kan nødvendig risikohåndtering oppnås gjennom reduksjons av avhengigheter til eksterne ressurser eller andre virksomheter, eksempelvis ved at virksomheten selv skaffer til veie de aktuelle ressursene eller ved hjelp av reserveløsninger.

I henhold til virksomhetsikkerhetsforskriften:

§ 13. Håndtering av risiko (andre ledd)

Virksomheten skal sende en oversikt over andre virksomheter den er avhengig av for å fungere som den skal, til Nasjonal sikkerhetsmyndighet og det departementet som er ansvarlig for det forebyggende sikkerhetsarbeidet i sektoren.

… skal virksomheten holde oversikt over avhengigheter og holde NSM og sektordepartementet informert om disse.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

post@nsm.stat.no
www.nsm.stat.no