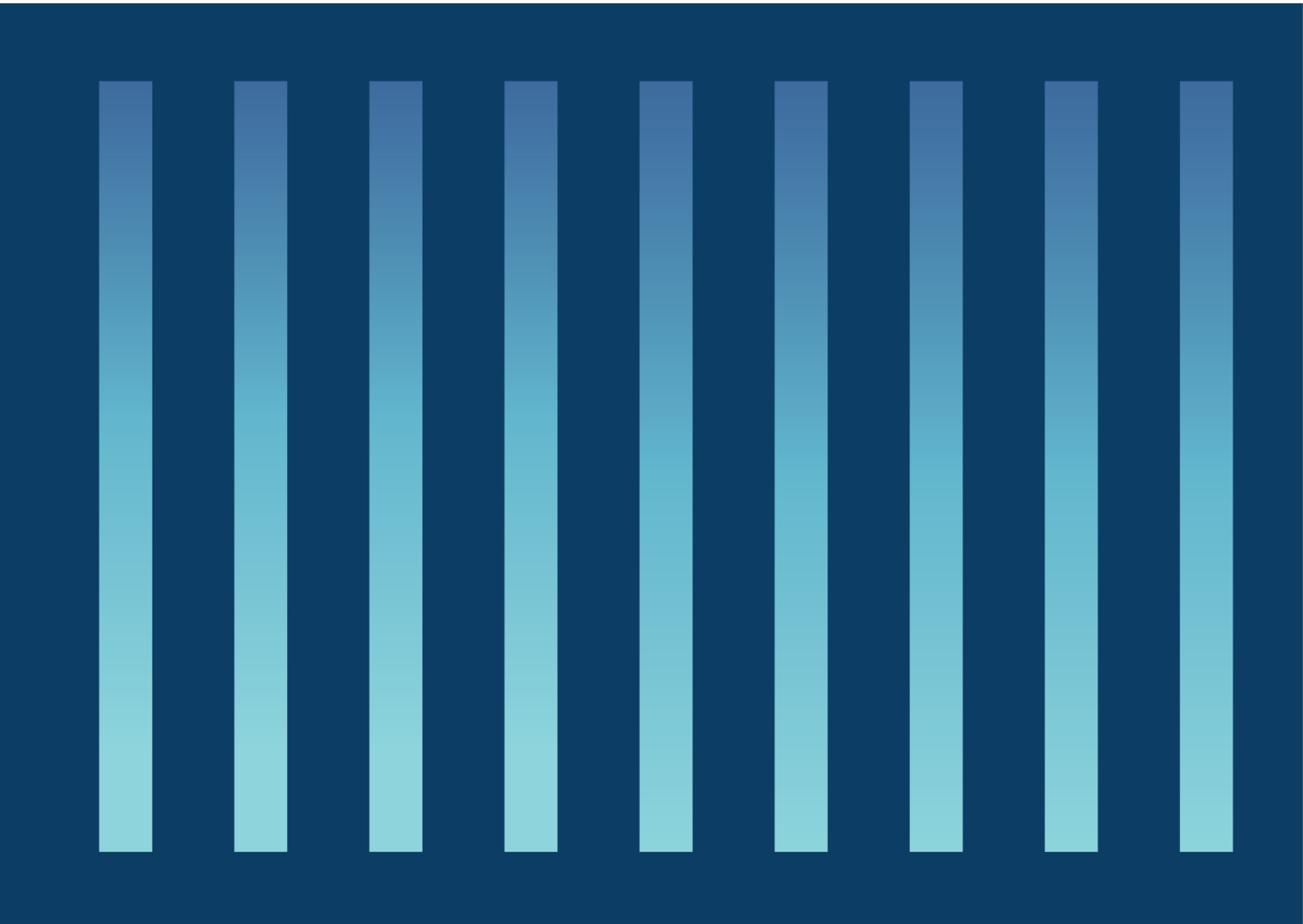
NASJONAL
SIKKERHETSMYNDIGHET

Veileder i sikkerhetsstyring

Versjon: 1



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 veiledninger 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. Sikkerhetsstyring

Målgruppen for *Veileder i sikkerhetsstyring* er virksomheter som skal etablere sikkerhetsstyring for forebyggende sikkerhet i samsvar med krav i eller i medhold av sikkerhetsloven

Sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Hva som er å anse som forsvarlig sikkerhet vil avhenge av virksomhetens skjermingsverdige verdier og akseptkriteriene knyttet til disse, kombinert med den aktuelle risikovurderingen. Da forsvarlig sikkerhet vil forandre seg over tid, på bakgrunn av endring av risiko, skal sikkerhetsstyring også ivareta prinsippet om kontinuerlig forbedring av sikkerhetsarbeidet i virksomheten.

1.1. Krav om sikkerhetsstyring

Sikkerhetsstyring omfatter alle aktiviteter med betydning for forebyggende sikkerhetsarbeid og skal gjennomføres planlagt og systematisk i form av et sikkerhetsstyringssystem som omfatter planlegging, etablering, gjennomføring og forbedring av det forebyggende sikkerhetsarbeidet. Sikkerhetsstyringen skal være del av virksomhetsstyringen for øvrig jf.:

> *§ 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 med krav om etablering av sikkerhetsstyringssystem i:

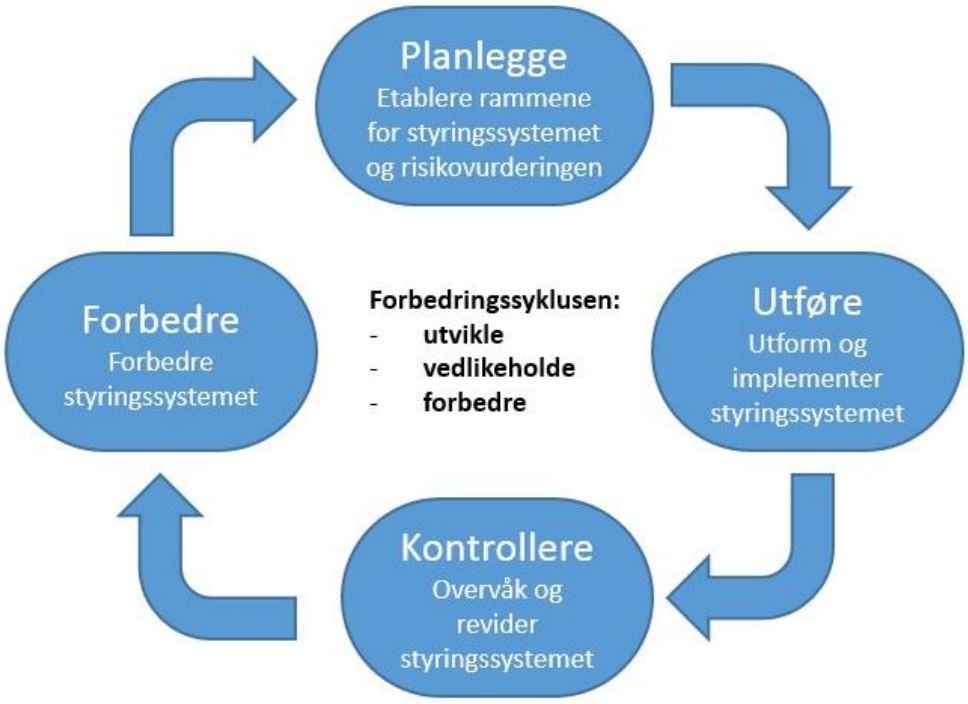
> *§ 3. Styringssystem for sikkerhet*
>
> *En virksomhet som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten oppfyller kravene gitt i eller med hjemmel i loven.*

Kravet om etablering av styringssystem for sikkerhet gjelder uavhengig av om virksomheten har en skjermingsverdig verdi. Sikkerhetsstyringssystemets utforming avhenger av de verdier som skal beskyttes og hvordan beskyttelsen etableres. Utformingen henger følgelig sammen med risiko for sikkerhetstruende virksomhet. NSM legger til grunn at styringssystemet for sikkerhet skal omfatte hele det forebyggende sikkerhetsarbeidet, det vil si både aktiviteter dedikert for sikkerhet og aktiviteter som kan ha betydning for sikkerhet. Dette innebærer at styringssystemet for sikkerhet skal omfatte:

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

- sikkerhetsdokumentasjon

Disse prinsippene for sikkerhetsstyring har sammenheng med grunnleggende forutsetninger for styring og kontinuerlig forbedring: Planlegge, utføre, kontrollere og forbedre – som illustrert i Figur 1.



Figur 1: Styring og kontinuerlig forbedring

Styringssystemet for sikkerhet skal samordnes med virksomhetsstyringen for øvrig. Dette vil gi grunnlag for felles tilnærming i håndteringen av de risikoer virksomheten står overfor. Med utgangspunkt i prinsippene for sikkerhetsstyring vil det være mulig å identifisere de deler av eksisterende virksomhetsstyring som kan utvides og tilpasses til også å dekke forebyggende sikkerhetsarbeid. Eksempelvis kan virksomhetens kompetansestyring utvides til også å omfatte sikkerhetskompetanse, og prosedyrer for avviksrapportering kan tilpasses til å inkludere rapporter om sikkerhetstruende virksomhet.

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.

Styringssystemet kan med fordel etableres med grunnlag i anerkjente standarder for styring som for eksempel ISO 9000-serien og ISO 27000-serien. Forutsetningen er at styringssystemet dekker (hele) det forebyggende sikkerhetsarbeidet, er dimensjonert i forhold til risiko for sikkerhetstruende virksomhet og oppfyller kravene i og i medhold av sikkerhetsloven, slik disse er beskrevet for hvert av styringselementene i kapittel 2-8 i denne veiledningen.

2. Risikostyring

Det overordnede målet for forebyggende sikkerhetsarbeid er å oppnå forsvarlig sikkerhetsnivå for de skjermingsverdige verdiene, jf. sikkerhetsloven § 4-3 og virksomhetssikkerhetsforskriften § 5.

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

Begrepet «forsvarlig sikkerhet» danner grunnlaget for hvordan virksomheten må sikre sine skjermingsverdige verdier. Hva som er forsvarlig sikkerhet for virksomheten, må vurderes opp mot virksomhetens skjermingsverdige verdier og funksjonskravene sikkerhetsloven stiller til disse.

For å hele tiden ha kontroll på virksomhetens verdier samt forsvarlig sikkerhetsnivå må virksomheten kontinuerlig vurdere risiko knyttet til virksomhetens skjermingsverdige verdier og håndtering av slik risiko. Dette er risikostyring.

Risikovurdering omfatter informasjon om verdier, identifisering av trusler og avdekking av sårbarheter. Avdekking av sårbarheter og identifisering av trusler kan gjennomføres med utgangspunkt i scenarioer som beskriver relevante uønskede hendelser. Scenarioene kan konkretiseres ytterligere ved å angi mulige aktører bak hendelsene, og dennes tilhørighet til virksomheten og kapasitet og intensjon til å forårsake hendelser. Risikovurderingen definerer hva som er forsvarlig sikkerhetsnivå for virksomheten og danner grunnlag for risikohåndteringen.

Risikohåndtering omfatter etablering av sikkerhetstiltak, tilpasset de skjermingsverdige verdier virksomheten forvalter, for å redusere sårbarhetene i nødvendig omfang. Forsvarlig sikkerhetsnivå oppnås dermed gjennom beskyttelse av de skjermingsverdige verdiene ved hjelp av sikkerhetstiltak.

2.1. Krav om risikovurderinger

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.*

Forebyggende sikkerhetsarbeid skal etableres med grunning i risikovurderinger. Slike vurderinger må følgelig gjennomføres ved hver 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 med betydning for virksomheten.

Virksomheten kan selv bestemme hvilke verdier og forhold som skal omfattes av den enkelte risikovurdering. 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 må omfatte:

- informasjon om skjermingsverdige verdier – blant annet i form av opplysninger om gradering og/eller klassifisering av disse verdiene
- 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 gradering og/eller klassifisering av skjermingsverdige verdier fremgår av virksomhetens verdivurderinger og/eller skadevurderinger. Disse skal kartlegge og rangere virksomhetens verdier med en vurdering av konsekvens dersom verdien kompromitteres, blir utilgjengelige, skades, ødelegges eller rettstridig overtas av andre.

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

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. Uønskede hendelser overfor avhengighetene er ikke avgrenset til tilsiktede handlinger. Risikovurderinger som dekker avhengigheter må derfor også omfatte scenarioer knyttet til utilsiktede hendelser.

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

2.1.1. Scenarioer

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

2.1.2. Aktører

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

2.1.2.1. Tilhørighet

- *eget personell*[1] *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* – dvs. medarbeidere i arbeidsforhold
- *eksternt personell* – som ikke har tilknytting til virksomheten

2.1.2.2. Kapasitet (eller evne)

- *liten* – grunnleggende kompetanse, kjennskap til funksjon og operativt miljø fra åpne kilder, allment tilgjengelige ressurser

[1] *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

- *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

2.1.2.3. Intensjon (eller vilje)

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

2.2. Krav om risikohåndtering

Virksomhetsikkerhetsforskriften har krav til håndtering av risiko 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.*

Bestemmelsen må forstås slik at sikkerhetsstyringssystemet skal dimensjoneres i forhold til risikoen overfor de skjermingsverdige verdiene. Med utgangspunkt i risikovurderinger etableres sikkerhetstiltak, der dette er nødvendig, for å redusere risiko til akseptabelt nivå slik at sikkerhetsnivået blir forsvarlig.

Sikkerhetstiltakene kan etableres for å:

- endre sårbarheten til skjermingsverdige verdier dvs. gjennom forsterket sikkerhet
- redusere konsekvensen av uønskede hendelser, eksempelvis gjennom redundans eller effektiv hendelseshåndtering
- redusere avhengigheter

Sikkerhetstiltak kan etableres som hensiktsmessige balanserte kombinasjoner av fysiske, elektroniske, organisatoriske og menneskelige tiltak, jf. kapittel 5 i denne veiledningen.

For å redusere avhengigheter kan det være nødvendig å sørge for redundans av kritiske tjenester som understøtter virksomhetens skjermingsverdige verdier.

Sikkerhetstiltak som etableres på bakgrunn 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.

2.2.1. Tiltaksvurdering for å oppnå forsvarlig sikkerhet

Hvorvidt allerede etablerte eller foreslåtte sikkerhetstiltak vil gi akseptabelt risikonivå og med dette forsvarlig sikkerhetsnivå, vurderes:

- for hvert av scenarioene det må beskyttes mot (se kapittel 2.1.1. foran)
- i forhold til gradering for berørt informasjon/klassifisering av berørt informasjonssystem, objekt eller infrastruktur

For å kunne ivareta forsvarlig sikkerhet må sikkerhetstiltakene kunne beskytte mot aktører, eget personell og eksterne, som har kapasitet og intensjon/vilje til å utføre sikkerhetstruende virksomhet, se kapittel 2.1.2 for beskrivelse av aktørene. Med kapasitet menes blant annet aktørens tilgjengelige ressurser til å gjennomføre sikkerhetstruende virksomhet.

Ettersom aktørens kapasitet og intensjon/vilje øker, må grunnsikringen økes tilsvarende, se kapittel 2.2.1.1 og 2.2.1.2. Det settes høyere krav til beskyttelse mot eksterne da disse ikke omfattes av den oppfølging som er mulig overfor eget personell. Vurdering av tiltak for å beskytte skjermingsverdig informasjon. 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.

	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**

Figur 2: Vurdering av tiltak for å beskytte skjermingsverdig informasjon

Leseveiledning til Figur 2:

BEGRENSET

Eget personell (med eller uten tilgang) skal ikke kunne forårsake uønskede hendelser overfor skjermingsverdig informasjon sikkerhetsgradert BEGRENSET dersom de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – gjennom 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 (middels kapasitet) – ved bevisst opportunistisk handling.

KONFIDENSIELT

Eget personell (med tilgang) skal ikke kunne forårsake uønskede hendelser overfor skjermingsverdig informasjon sikkerhetsgradert KONFIDENSIELT dersom de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – gjennom 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 (middels kapasitet) – 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 (stor kapasitet) – med hensikt og plan.

HEMMELIG

Eget personell (med tilgang) skal ikke kunne forårsake uønskede hendelser overfor skjermingsverdig informasjon sikkerhetsgradert HEMMELIG selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser (middels kapasitet) – 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 (stor kapasitet) – med hensikt og plan.

STRENGT HEMMELIG

Det skal ikke være mulig å forårsake uønskede hendelser overfor skjermingsverdig 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.

Eksempler på vurdering av sikkerhetstiltak i Figur 2:

BEGRENSET

Situasjon: Skriver er tilkoblet informasjonssystem for behandling av informasjon sikkerhetsgradert BEGRENSET er plassert i der både medarbeidere med og uten autorisasjon for tilgang til informasjon sikkerhetsgradert BEGRENSET har adgang. Dokumenter skrives ut straks de sendes til utskrift. Virksomhetens sikkerhetsinstruks har ikke regler om håndtering av utskrifter.

Scenario: Medarbeidere (med eller uten tilgang) tar ved feil med seg (deler av) andres utskrifter med sikkerhetsgradert informasjon, og sender disse (sammen med eget dokument) ut av virksomheten.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at egne medarbeidere (med eller uten) tilgang, ubevisst kan kompromittere informasjon sikkerhetsgradert BEGRENSET. Sikkerhetsnivået er følgelig ikke forsvarlig.

KONFIDENSIELT

Situasjon: I et åpent kontorlandskap, etablert som beskyttet sone, har en virksomhet innleid renholdspersonell. Virksomheten har et informasjonssystem for behandling av informasjon sikkerhetsgradert KONFIDESIELT i sonen. Informasjonssystemets har ikke automatisk skjermsparer og låsing av PC og sikkerhetsinstruksen har ikke regler som beskriver bruk av skjermsparer og låsing.

Scenario: Innleid renholdspersonell (eget personell uten tilgang) blir fulgt av personer med permanent adgang, men får ved gjennomføring av renholdet allikevel innsyn i informasjon på PC-skjermer til brukere som har forlatt arbeidsstasjonen.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at egne medarbeidere uten tilgang, bevisst og opportunistisk kan tilegne seg informasjon sikkerhetsgradert KONFIDENSIELT. Sikkerhetsnivået er følgelig ikke forsvarlig.

HEMMELIG

Situasjon: En virksomhet som behandler sikkerhetsgradert informasjon HEMMELIG har ikke sikrede rom eller lokaler for tale sikkerhetsgradert HEMMELIG. Virksomhetens lokaler er etablert i et forretningsbygg med flere andre eksterne virksomheter i tilstøtende lokaler.

Virksomheten har ikke oversikt over hvilke aktører som har tilgang til tilstøtende lokaler. Når virksomheten behandler og diskuterer informasjon sikkerhetsgradert HEMMELIG gjøres dette på dedikert kontor og sikkerhetsinstruksen har regler som beskriver at alt av elektronisk utstyr ikke skal medbringes inn i rommet.

Scenario: Statlig trusselaktør (eksterne) disponerer etasjen over virksomhetens lokaler. Trusselvurderinger konkluderer med at den statlige trusselaktøren har en interesse i informasjon virksomheten besitter.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at eksterne, med hensikt, plan og tilpasset kompetanse kan kompromittere informasjon sikkerhetsgradert HEMMELIG. Sikkerhetsnivået er følgelig ikke forsvarlig.

STRENGT HEMMELIG

Situasjon: Informasjonssystem for behandling av informasjon sikkerhetsgradert STRENGT HEMMELIG er plassert i sperret område og for bruk av en (autorisert og sikkerhetsklarert) medarbeider av gangen. Systemet har ingen eksterne tilkoblinger eller flyttbare lagringsmedier, men mulighet for kopiering av sikkerhetsgradert informasjon til flyttbart lagringsmedium.

Scenario: Egne medarbeidere med tilgang til det aktuelle informasjonssystemet kan kopiere sikkerhetsgradert informasjon til medbrakt flyttbart lagringsmedia og ta informasjonen med ut av virksomheten.

Vurdering: Gjeldende sikkerhetsnivå muliggjøre at egne medarbeidere med tilgang og med hensikt og plan kan kompromittere informasjon sikkerhetsgradert STRENGT HEMMELIG. Sikkerhetsnivået er følgelig ikke forsvarlig.

2.2.1.1. Vurdering av tiltak for å beskytte skjermingsverdig objekt eller infrastruktur

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 enn konfidensialitet. Vurderingen gjennomføres da i forhold til klassifiseringen for objekter eller infrastruktur som berøres dersom informasjon går tapt, blir endret eller blir utilgjengelig.

	EGET PERSONELL MED TILGANG	EGET PERSONELL UTEN TILGANG	EKSTERNE	FREKVENS[2]
UNDERSTØTTER[3]	**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**

Figur 3: Vurdering av tiltak for å beskytte skjermingsverdig informasjonssystem, infrastruktur eller objekt

[2] Sannsynlighet for bortfall

[3] 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.

Leseveiledning til Figur 3:

UNDERSTØTTER

Eget personell (med eller uten tilgang) skal ikke kunne forårsake uønskede hendelser som påvirker funksjon i informasjonssystem som UNDERSTØTTER skjermingsverdig objekt, eller infrastruktur, dersom de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – gjennom 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 (middels kapasitet) – ved bevisst opportunistisk handling.

VIKTIG

Eget personell (med tilgang) skal ikke kunne forårsake uønskede hendelser som påvirker funksjon i informasjonssystem[4], objekt eller infrastruktur som er klassifisert VIKTIG dersom de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – gjennom 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 (middels kapasitet) – 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 (stor kapasitet) – med hensikt og plan.

KRITISK

Eget personell (med tilgang) skal ikke kunne forårsake uønskede hendelser som påvirker funksjon i informasjonssystem[5], objekt eller infrastruktur klassifisert KRITISK, selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser (middels kapasitet) – 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 (stor kapasitet) – med hensikt og plan.

MEGET KRITISK

Eget personell (med eller uten tilgang) skal ikke kunne forårsake uønskede hendelser som påvirker funksjon i informasjonssystem[5], objekt eller infrastruktur klassifisert MEGET KRITISK, selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser (stor kapasitet) – med hensikt og plan.

Eksempler på vurdering av sikkerhetstiltak i Figur 3:

UNDERSTØTTER

Situasjon: Virksomheten har medarbeidere med tilganger til informasjonssystem som understøtter en skjermingsverdig verdi. Virksomheten har ikke regler for oppdatering av tilgangsstyring og påloggingsrutiner, når ansatte slutter.

Scenario: Tidligere ansatte (eksterne) benytter gammel påloggingsdata og kjennskap til virksomhetens rutiner for å få tilgang til informasjonssystemet, og kan med dette forårsake uønskede hendelser overfor den skjermingsverdige verdien.

[4] Informasjonssystem som selv er klassifisert eller som har avgjørende betydning for klassifisert objekt eller infrastruktur.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at eksterne med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser, bevisst kan påvirke funksjonen i informasjonssystemet. Sikkerhetsnivået er følgelig ikke forsvarlig.

VIKTIG

Situasjon: Tjener i informasjonssystem klassifisert VIKTIG er plassert i felles serverrom der også driftspersonell uten tjenstlig (kun med behov knyttet til den aktuelle tjeneren) har adgang.

Scenario: Medarbeidere uten tilgang til det aktuelle informasjonssystemet kan gjennom adgang til serverrommet forårsake driftsavbrudd for tjeneren i det klassifiserte informasjonssystemet.

Vurdering: Gjeldende sikkerhetsnivå muliggjøre at egne medarbeidere uten tilgang og som (gjennom sin stilling) har utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser, bevisst kan påvirke funksjonen i informasjonssystem som er klassifisert VIKTIG. Sikkerhetsnivået er følgelig ikke forsvarlig.

KRITISK

Situasjon: Medarbeidere med tilgang til informasjonssystem klassifisert KRITISK har rettigheter for bruk av systemet utover tjenstlig behov.

Scenario: Medarbeidere med tilgang til det aktuelle informasjonssystemet kan benytte utvidede rettigheter for bruk av systemet til uønsket modifikasjon av data og til å hindre registrering av bruk av systemet.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at egne medarbeidere med tilgang og med tilpassede ressurser (gjennom utvidede rettigheter), bevisst kan påvirke funksjonen i informasjonssystem som er klassifisert KRITISK. Sikkerhetsnivået er følgelig ikke forsvarlig.

MEGET KRITISK

Situasjon: Datasenter klassifisert MEGET KRITISK er plassert i et eget avlåst lokale i en fjellhall hvor også andre virksomheter leier lokaler. Fjellhallen eies og driftes av et privat aksjeselskap som har ansvar for vakthold, drift og leveranse av strøm og kjøling. Alle virksomhetene som er lokalisert i fjellhallen har selvstendig tilgang til felles kjøle- og strømanlegg.

Scenario: Personell fra andre virksomheter kan forårsake svikt i kjøle- eller strømanlegg.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at eksterne med tilpasset kompetanse, nødvendige ressurser og med hensikt og plan vil kunne forårsake uønskede hendelser overfor skjermingsverdig objekt klassifisert MEGET KRITISK. Sikkerhetsnivået er følgelig ikke forsvarlig.

2.2.2. Avhengigheter

I den grad virksomheten er avhengig av (eksterne) ressurser/andre virksomheter for å håndtere og beskytte skjermingsverdigeverdier, må også slike forhold dekkes av risikohåndteringen. Nødvendig risikohåndtering kan oppnås gjennom sikring av eksterne ressurser eller andre virksomheter som virksomheten er avhengig av, eller reduksjons av avhengigheter til disse. Reduksjon av avhengigheter kan eksempelvis gjøres ved at virksomheten selv skaffer til veie de aktuelle ressursene eller ved hjelp av reserveløsninger. Virksomheten skal holde oversikt over avhengigheter og holde NSM og sektordepartementet informert om disse.

3. Sikkerhetsledelse

Virksomhetens leder har det endelige ansvaret for det forebyggende sikkerhetsarbeidet og for at dette arbeidet gir forsvarlig sikkerhet som resultat. «Virksomhetens leder» må tolkes i lys av ansvarsfordelingen som fremgår av forvaltningsretten for offentlige virksomheter og selskapsretten for private virksomheter. Ansvaret omfatter forebyggende sikkerhetsarbeid i virksomheten og sikkerhetsarbeid knyttet til aktiviteter utført av andre for virksomheten.

Ansvaret innebærer utøvelse av sikkerhetsledelse. Dette omfatter fastlegging av prinsipper for forebyggende sikkerhetsarbeid, fordeling av ansvar og myndighet for gjennomføring av arbeidet, tilrettelegging for slik gjennomføring og oppfølging av det forebyggende sikkerhetsarbeidet.

Sikkerhetsloven stiller krav til sikkerhetsledelse i:

§ 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.

Forebyggende sikkerhetsarbeid er et lederansvar som forutsetter sikkerhetsledelse gjennom overordnede føringer om:

- verdier som må beskyttes – eksempelvis skjermingsverdig informasjon med tilhørende gradering 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

Føringene beskrives kort og overordnet i virksomhetens styringsdokument for forebyggende sikkerhetsarbeid. Styringsdokumentet tjener som informasjon fra virksomhetens ledelse til ansatte i virksomheten og underleverandører om forpliktelser og forventninger i det forebyggende sikkerhetsarbeidet. Informasjon om virksomhetens sikkerhetsarbeid deles etter tjenstlig behov.

Styringsdokument for forebyggende sikkerhetsarbeid

Virksomheten har ansvar for [objekt] som iht. sikkerhetsloven er et skjermingsverdig objekt. Objektet er klassifisert som KRITISK. Virksomheten behandler informasjon som er skjermingsverdig iht. sikkerhetsloven skjermingsverdige objektet. Informasjonen er sikkerhetsgradert inntil HEMMELIG.

Objekt og informasjon er sikret iht. krav om sikring av hhv skjermingsverdig objekt og skjermingsverdig informasjon gitt i eller i medhold av sikkerhetsloven.

Ansvar og myndighet for det forebyggende sikkerhetsarbeidet er fordelt slik at ledelsen har det endelige ansvaret for sikkerhetsarbeidet, linjeledere er ansvarlig for sikkerhetsarbeidet innen sitt myndighetsområde og hver medarbeider har ansvar for at egen arbeidsutførelse er sikker og som besluttet. Virksomhetens leder har utpekt en Sikkerhetsleder som bistår i det forebyggende sikkerhetsarbeidet og har særlige oppgaver knyttet til hendelseshåndtering, sikkerhetsrevisjon og ledelsens årlige gjennomgang av arbeidet.

Sikring er etablert med utgangspunkt i skadevurdering og trusselvurdering. Disse vurderingene oppdateres etter behov og minst årlig i form av en helhetlig risikovurdering for virksomheten. I tillegg gjennomføres avgrensede risikovurderinger ved alle endringer – eksterne eller interne – som kan påvirke sikkerheten. De operative risikovurderingene benyttes som grunnlag for valg og etablering av sikkerhetstiltak.

Forbyggende sikkerhetsarbeid gjennomføres som sikkerhetsstyring. Sikkerhetsstyringen er del av virksomhetens samlede virksomhetsstyring og gjennomføres iht. allment akseptert standard for sikkerhetsstyring og NSMs grunnprinsipper for IKT-sikkerhet. Bl.a. gjennomføres jevnlige sikkerhetsrevisjoner og årlige gjennomganger av de forebyggende sikkerhetsarbeidet.

Boks 1: Eksempel på innhold i styringsdokument for forebyggende sikkerhet

3.1. Ressurser og kompetanse

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

§ 7. Ressurser og kompetanse (første ledd)

En virksomhet skal forvalte og utvikle det forebyggende sikkerhetsarbeidet sitt på en forsvarlig måte.

Bestemmelsen må forstås slik at sikkerhetsledelse også omfatter å legge til rette for gjennomføring av forebyggende sikkerhetsarbeid. Slik tilrettelegging omfatter tildeling av nødvendige ressurser, ikke kun økonomiske ressurser, men også tilstrekkelig tid og nødvendige verktøy, for å gjennomføre arbeidet med forsvarlig sikkerhet som resultat.

4. Sikkerhetsorganisering

Sikkerhetsorganisering omfatter fordeling av ansvar og myndighet for utførelse av arbeidsoppgaver, klargjøring av forutsetninger og plikter for den enkeltes arbeidsutførelse og tilrettelegging gjennom informasjon, opplæring og vedlikehold av kompetanse for denne utførelsen.

Sikkerhetsarbeidet organiseres med utgangspunkt i at virksomhetens ledelse beslutter, (linje-) organisasjonen utfører og melder fra, og dedikerte roller bistår og følger opp det forebyggende sikkerhetsarbeidet. Sikkerhetsorganiseringen omfatter alle som utfører aktiviteter med betydning for sikkerhet (og ikke kun de dedikerte rollene).

4.1. Krav om sikkerhetsorganisering

Sikkerhetsloven har krav om sikkerhetsorganisering i:

§ 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 sikkerhetene

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

Alle som gjennomfører aktiviteter med betydning for sikkerhet må ha nødvendig informasjon om risiko for sikkerhetstruende virksomhet og om sikkerhetsstyringssystemet, samt kjenne de grunnleggende forutsetningene for egen arbeidsutførelse. Videre må den enkelte kjenne til eget ansvar, egen myndighet og hvordan aktivitetene skal utføres. Slik informasjon gis eksempelvis i rollebeskrivelser.

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

4.2. 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 vil omfatte aktiviteter knyttet til beslutninger, utførelse og oppfølging. Ansvar og myndighet for disse aktivitetene må være fordelt til rollene som skal gjennomføre dem. Virksomhetens ledelse beslutter overordnede føringer for forebyggende sikkerhetsarbeid og følger opp arbeidet. Linjeledere er ansvarlig for sikkerhetsarbeidet innen sitt myndighetsområde og hver medarbeider har ansvar for at egen arbeidsutførelse er sikker og som besluttet. I tillegg kan virksomheten utpeke enkelte roller med dedikerte oppgaver i det forbyggende sikkerhetsarbeidet.

Antall og typer roller som etableres må sees i sammenheng med de skjermingsverdige verdiene virksomheten råder over og omfanget av disse. Som minimum er det aktuelt å fordele ansvar og myndighet for å følge opp og bistå det forebyggende sikkerhetsarbeidet til roller som bistår ved, og påser gjennomføring av arbeidsoppgaver med betydning for sikkerhet. Eksempelvis kan det være behov for funksjonen sikkerhetsleder. I virksomheter med utstrakt bruk av informasjonsteknologi kan det være behov for en IKT-sikkerhetsleder.

Utførelse av forebyggende sikkerhetsarbeid, og oppfølging av dette arbeidet må skje uavhengig av hverandre, blant annet slik at ikke medarbeidere settes til å kontrollere egen arbeidsutførelse.

Eksempler på oppgaver for sikkerhetsleder:

- bidra til bevisstgjøring og kompetansebygging innen sikkerhet i virksomheten
- gi råd om forebyggende sikkerhetsarbeid, inkl. risikohåndtering
- ha oversikt over de skjermingsverdige verdier virksomhetene håndterer
- koordinere hendelseshåndtering og gi råd om korrigerende tiltak
- orientere virksomhetsledelsen om oppfølging av avvik og sikkerhetstruende hendelser
- evaluere sikkerhetsstyringssystem, ev. gjennom sikkerhetsrevisjoner
- forberede og referatføre ledelsens gjennomgang av det forebyggende sikkerhetsarbeidet

4.3. Taushetsplikt

Sikkerhetsloven har krav om taushetsplikt:

> *§ 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.*

Langt de fleste som utfører oppgaver med betydning for forebyggende sikkerhet vil ha tilgang til sikkerhetsgradert informasjon. Dette innebære at taushetsplikt gjelder for alle medarbeidere og alle andre som utfører arbeid med betydning for virksomhetens sikkerhetsarbeid. Disse skal informeres om den taushetsplikt som gjelder, herunder at taushetsplikten gjelder også etter at arbeidet eller tjenesten er avsluttet. Informasjonen skal omfatte opplysninger om pliktens omfang, varighet og konsekvensene dersom det brytes.

Medarbeidere og andre skal bekrefte at taushetsplikten er kjent og forstått i taushetserklæring som oppbevares av virksomheten.

4.4. Sikkerhet ved fratredelse

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

> *§ 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.*

Ved endringer i arbeidsforholdet skal tilgang til skjermingsverdig verdier endres i samsvar med nye tjenstlige behov. Det betyr at når medarbeidere slutter skal virksomheten sørge for at den som fratrer ikke lenger har tilgang til verdiene. Taushetsplikten gjelder også etter medarbeideren har sluttet.

5. Sikkerhetstiltak

Verdier skal beskyttes slik at risiko for sikkerhetstruende virksomhet reduseres til akseptabelt nivå. Risikoreduksjon oppnås gjennom etablering av menneskelige, fysiske, elektroniske og/eller organisatoriske sikkerhetstiltak.

Sikkerhetstiltak og -prosedyrer etableres som balansert sikring i form av barrierer, deteksjon, verifikasjon og reaksjon. Sikringen må etableres slik at det tar lenger tid å gjennomføre en uønsket hendelse (eks. innbruddstid) enn det tar å håndtere den Dette betegnes "positivt tidsregnskap".

5.1. Krav om sikkerhetstiltak

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 skjermingsverdige verdien.

Sikkerhetstiltak etableres med grunnlag i vurdering av risiko for sikkerhetstruende virksomhet, slik at risiko reduseres til akseptabelt nivå og sikkerhetsnivået blir forsvarlig.

Grunnsikring etableres basert på vurdering av risiko for sikkerhetstruende virksomhet i normaltilstanden. Grunnsikringstiltakene skal fungere slik at frafallet av ett tiltak ikke påvirker den totale sikringsevnen. Virksomheten velger selv den mest hensiktsmessige kombinasjon av tiltak basert på vurdering av risiko. Dette gjelder både hvorvidt tiltakene er utformet fysisk, elektronisk,

menneskelig eller organisatorisk og hvilken funksjon de har (barriere, deteksjon, verifikasjon og reaksjon).

Kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket, men tiltak må etableres når dette er nødvendig for å oppnå et forsvarlig sikkerhetsnivå. Kostnadseffektivitet kan ikke gå foran behovet for forsvarlig sikkerhetsnivå.

5.2. 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 påbyggingstiltakene 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.

5.3. Prinsipper for valg av sikkerhetstiltak

Virksomhetsikkerhetsforskriften angir prinsipper for valg og utforming av sikkerhetstiltak i:

> *§ 15 Prinsipper ved valg og utforming av sikkerhetstiltak*
>
> *Når en virksomhet velger ut og utformer sikkerhetstiltak, skal følgende prinsipper legges til grunn:*
>
> *a) Sikkerhetstiltakene skal ikke ha en annen funksjonalitet eller større kompleksitet enn nødvendig.*
>
> *b) Det skal ikke gis en mer omfattende tilgang til skjermingsverdige verdier enn nødvendig.*
>
> *c) Svikt i ett 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.

En virksomhet skal ikke bruke mer inngripende sikkerhetstiltak enn nødvendig for å håndtere en aktuell risiko. Virksomheten skal her særlig ta hensyn til enkeltpersoners rettssikkerhet og personvern. Det skal ikke behandles personopplysninger i større grad enn det som er nødvendig ut fra formålet med sikkerhetstiltaket.

Formålet er etablering av sikkerhetstiltak og -prosedyrer som samlet gir et forsvarlig sikkerhetsnivå. Tiltakene må virke etter sin hensikt, og effektiv sikring handler om å få mennesker, teknologi og organisasjon til å spille sammen på en god måte. Prinsippene angitt i virksomhetsikkerhetsforskriften § 15 må forstås å omfatte krav om:

a) *minimalisme* – Virksomheten må påse at det ikke velges løsninger med unødig funksjonalitet og kompliserte styringsmekanismer, som i verste fall kan føre til en forringelse av sikkerheten.

b) *minste privilegium* – Hensikten med å styre tilgangen til en skjermingsverdig verdi, er å hindre at personer uten tjenstlig behov får tilgang. Det skal ikke gis mer omfattende tilgang enn det som strengt tatt er nødvendig for å ivareta en funksjon, eller for å gi tilgang til informasjon.

c) *sikring i dybden* – En skjermingsverdig verdi må beskyttes på en slik måte at verdien ikke blir kompromittert selv om det kan være svikt i ett enkelt tiltak. For å kunne sikre dette er det viktig at man etablerer sikring i dybden, ved å etablere flere lag med fysiske, elektroniske, menneskelige og organisatoriske barrierer mellom usikret område og de verdiene man ønsker å sikre.

d) *motstandsdyktighet* – Tiltakene som iverksettes skal i minst mulig grad være avhengige av hverandre, slik at de ikke kan svekkes eller settes ut av funksjon samtidig med samme type handling. For å kunne sikre dette er det viktig at man sikrer verdiene både med barrierer, deteksjon, verifikasjon og reaksjon.

e) *balansert styrke* – Virksomhetens skjermingsverdige verdier, med likt sikkerhetsbehov, kan sikres med ulike tiltak, så fremt de oppnår samme effekt.

6. Forholdet til andre virksomheter

Ansvar og myndighet for forebyggende sikkerhetsarbeid må avklares med leverandører, samarbeidsparter og andre som kan påvirke virksomhetens skjermingsverdige verdier.

6.1. Krav knyttet til forholdet til andre virksomheter

Sikkerhetsloven har krav om forholdet til andre virksomheter i:

§ 4-1. Sikkerhetsstyring (annet ledd første setning)

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

Alle som gjennomfører aktiviteter med betydning for sikkerhet må kjenne forutsetningene og forpliktelsene knyttet til egen arbeidsutførelse. Virksomheten må gi den enkelte nødvendig informasjon om risiko for sikkerhetstruende virksomhet og om sikkerhetsstyringssystemet.

Bestemmelsen må forstås som et krav om at også andre (enn virksomhetens egne medarbeidere), som utfører aktiviteter med betydning for sikkerhet, må ha nødvendig tilgang til styringsdokumenter og informasjon om den enkeltes ansvar, myndighet og hvordan aktivitetene skal utføres. Eksempelvis må en underleverandør, håndverkere, vareleverandør eller datatekniker, kjenne de bestemmelser og og rutiner for adgang til områder og systemer som gjelder.

Forholdet til andre leverandører/samarbeidspartnere kan formaliseres i en leverandøravtale med sikkerhetsvilkår.

Sikkerhetsvilkår i leverandøravtale

Virksomheten er ansvarlig for at leverandørens personell får nødvendig risiko- og sikkerhetsopplæring. Det skal videre gis innføring i sikkerhetsprosedyrer som gjelder den enkeltes arbeid ved virksomheten, eksempelvis rapportering av sikkerhetstruende hendelser.

Virksomheten er ansvarlig for at leverandørens personell følger risiko- og sikkerhetsopplæring som er gitt og er gjeldende ved enhver tid.

Virksomheten har det daglige sikkerhetsmessige ansvaret for alt personell og det skal til enhver tid være tydelig hvem som har det overordnede sikkerhetsmessige ansvaret.

Virksomheten skal påse at innleid personell ikke gis tilgang til annen sikkerhetsgradert informasjon enn det som er nødvendig for gjennomføring av arbeidsoppdraget.

Leverandøren er ansvarlig for at leverandørens personell innehar nødvendig klarering.

Virksomheten som leier inn må kontrollere at innleid personell innehar nødvendig sikkerhetsklarering.

Virksomheten er ansvarlig for å gjennomføre autorisasjonssamtale med innleid personell.

Informasjon som tilfaller leverandørens personell som ledd i sitt arbeid hos virksomheten, skal ikke medbringes tilbake til leverandøren. Det skal heller ikke deles med personer uten tjenstlig behov eller andre personer utenfor virksomheten. Avvik fra dette anses som vesentlig mislighold fra avtalen og kan være grunnlag for heving.

Boks 2 Eksempel på sikkerhetsvilkår i leverandøravtale

7. Sikkerhetsoppfølging

Sikkerhetsoppfølging gjennomføres som håndtering av hendelser, evaluering og ledelsens gjennomgang av sikkerhetsstyringssystemet. Det kan i tillegg være aktuelt å kontrollere utførelsen av enkeltaktiviteter i sikkerhetsstyringssystemet, eksempelvis gjennom undersøkelser av registreringer fra arbeidsutførelsen i form av logger fra bruk av informasjonssystemene. Slike kontroller kan være grunnlag for deler av oppfølgingen, eller kan etableres som verifikasjonstiltak eksempelvis som del av øvelse hvor virksomhetens beredskapssystemer og adgangskontrollrutiner gjennomgås.

7.1. Krav om sikkerhetsoppfølging

Sikkerhetsloven har krav om sikkerhetsoppfølging i:

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

Bestemmelsen, sett i sammenheng med kravene i virksomhetsikkerhetsforskriften §§ 8, 9 og 10 må forstås slik at forebyggende sikkerhetsarbeid skal gjennomføres i en kontinuerlig forbedringsprosess med sikkerhetsoppfølging gjennom hendelseshåndtering, årlig evaluering og ledelsens gjennomgang.

7.1.1. Håndtering av uønskede hendelser[5]

Krav om sikkerhetsoppfølging er utdypet gjennom krav til håndtering av uønskede hendelser, i virksomhetsikkerhetsforskriften:

> *§ 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.

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

[5] Virksomheters håndtering av uønskede hendelser er beskrevet i egen veileder fra NSM.

7.1.2. Årlig evaluering

Virksomhetsikkerhetsforskriften har krav om evaluering av det forebyggende sikkerhetsarbeidet i:

> *§ 9. Evaluering og øvelser*
>
> *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.*
>
> *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.*
>
> *Resultatet av evalueringer og øvelser skal inngå i den årlige gjennomgangen av det forebyggende sikkerhetsarbeidet i virksomheten.*

Evaluering av oppfyllelse av krav om forsvarlig sikkerhetsnivå og sikkerhetsstyringssystemets egnethet skal gjennomføres som periodisk (årlig) undersøkelse.

Evalueringen kan med fordel gjennomføres i form av revisjon av sikkerhetsstyringssystemet. 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.

Bestemmelsene i, eller i medhold av, sikkerhetsloven og virksomhetens sikkerhetsstyringssystem er kriteriene det revideres etter. Manglende samsvar med revisjonskriteriene, dvs. avvik, korrigeres ved hendelseshåndtering som beskrevet over. Revisjonsresultatene rapporteres i tillegg som del av grunnlaget for ledelsens gjennomgang.

7.1.3. Ledelsens gjennomgang

Virksomhetsikkerhetsforskriften har krav om ledelsens gjennomgang av det forebyggende sikkerhetsarbeidet:

> *§ 10. Gjennomgang av det forebyggende sikkerhetsarbeidet av virksomhetens leder*
>
> *Leder 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.*

Ledelsens gjennomgang av det forebyggende sikkerhetsarbeidet skal avklare hvorvidt det er behov for endringer i sikkerhetsstyringssystemet. Endringsbehovet kan skyldes at systemet ikke fungerer som forutsatt, at det er gjort endringer internt i virksomheten, eller at virksomheten påvirkes av endringer i risiko eller føringer som følge av eksterne forhold.

Ledelsens gjennomgang er et årlig møte som oppsummerer årets forebyggende sikkerhetsarbeid og legger grunnlaget for forbedringsprosessen fremover. Møtet ledes av virksomhetens leder og alle øvrige ledere som påvirker eller kan påvirkes av sikkerhetsstyringssystemet deltar.

Grunnlag for møtet er informasjon om siste års forebyggende sikkerhetsarbeid, bl.a. fra hendelseshåndtering og revisjoner, samt informasjon om endringer (interne og eksterne) som kan påvirke det forebyggende sikkerhetsarbeidet. Ledelsens gjennomgang avsluttes med virksomhetens beslutning om eventuelle endringer i sikkerhetsstyringssystemet.

Agenda – ledelsens gjennomgang
1) Status for iverksetting av beslutninger fra forrige ledelsens gjennomgang
2) Status for måloppnåelse
3) Hendelser og resultater fra hendelseshåndtering siden forrige gjennomgang
4) Resultater fra og håndtering av interne sikkerhetsrevisjoner siden forrige gjennomgang
5) Resultater fra og håndtering av eksterne revisjoner og tilsyn siden forrige gjennomgang
6) Eksterne endringer som kan påvirke forebyggende sikkerhetsarbeid
7) Interne endringer som kan påvirke forebyggende sikkerhetsarbeid
8) Beslutninger om endringer i det forebyggende sikkerhetsarbeidet.

Boks 3 Eksempel på agenda for ledelsens gjennomgang

8. Sikkerhetsdokumentasjon

Sikkerhetsstyringssystemet må være tilstrekkelig dokumentert. Hvordan arbeidet skal utføres og kontrolleres skal fremkomme i dokumentasjonen. Dokumentasjonen må tilpasses virksomhetens verdier mht. krav til forebyggende sikkerhet og virksomhetens behov. Dokumentasjonen må oppdateres jevnlig.

8.1. Krav om sikkerhetsdokumentasjon

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 gjennom krav til sikkerhetsdokumentasjon i virksomhetsikkerhetsforskriften:

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

Bestemmelsen må forstås slik at 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 kan 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, rapporter fra håndtering av uønskede hendelser og evaluering og referater fra ledelsens gjennomgåelse.

8.2. Beskyttelse av sikkerhetsdokumentasjon

Sikkerhetsloven og virksomhetsikkerhetsforskriften har i tillegg bestemmelser om beskyttelse av skjermingsverdig informasjon. Disse kan også ha betydning for sikkerhetsdokumentasjon, men omtales ikke nærmere i denne veiledningen

.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

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