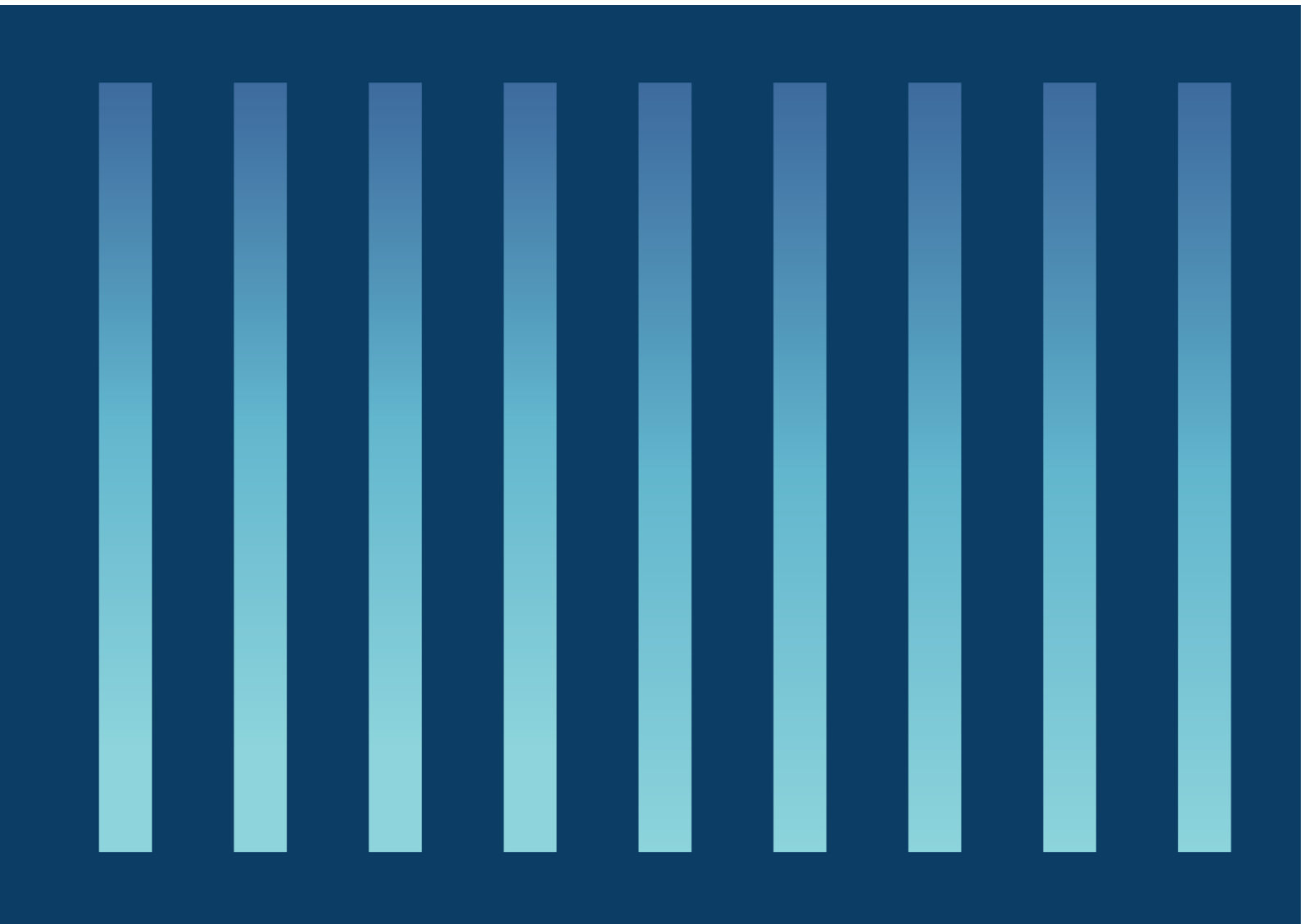
NASJONAL
SIKKERHETSMYNDIGHET

Veileder i fysisk sikkerhet

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. Innledning

1.1. Målgruppe

Målgruppen for veilederen er alle virksomheter som omfattes av sikkerhetsloven.

1.2. Formål

Veilederen skal gi råd og anbefalinger om hvilke forhold virksomheten må ta hensyn til ved valg av fysiske sikkerhetstiltak for å sikre et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier. Ny sikkerhetslov gjeldende fra 1.1.2019 har en funksjonell tilnærming for valg av sikkerhetstiltak som gir virksomhetene fleksibilitet til selv å velge tilstrekkelige sikkerhetstiltak ut fra egen risikovurdering. Krav til forsvarlig sikkerhetsnivå skal ikke fravikes. Hva som til enhver tid er faglig forsvarlig, endrer seg. Dette henger sammen med teknologiske forandringer og nyvinninger, og endringer i trussel- og risikobildet.

I denne veilederen brukes sikkerhet som et overordnet mål eller tilstand som innebærer fravær av uønskede hendelser, frykt eller fare. All aktivitet for å oppnå sikkerhet er sikring. Sikkerhetslov og tilhørende forskrifter benytter begrepet sikkerhetstiltak for tiltak som skal redusere sårbarhet, og dermed risiko, forbundet med uønskede handlinger. Veilederen benytter således samme begrep, men kan sidestilles med begrepet sikringstiltak.

Risikovurderingen skal konkludere med hvordan virksomheten skal håndtere den risikoen som er avdekket, og herunder hvilken grad av risiko som kan aksepteres. Sikkerhetstiltakene avgjøres på bakgrunn av disse akseptkriteriene. Det vises her til Veileder i sikkerhetsstyring. God sikkerhetskompetanse er avgjørende for å kunne oppnå et forsvarlig sikkerhetsnivå.

Det settes en nedre grense for hva som vurderes å være et forsvarlig sikkerhetsnivå i forhold til virksomhetens skjermingsverdige verdier. Objekter, infrastruktur og informasjonssystemer er skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner dersom de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse, eller rettstridig overtakelse, ref. sikkerhetsloven § 7-1. Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjon blir kjent for uvedkommende, går tapt, blir endret, eller blir utilgjengelig. Sikkerhetsgradert informasjon er skjermingsverdig informasjon som har blitt påført en sikkerhetsgradering etter sikkerhetsloven § 5-3 hvis det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Skjermingsverdig informasjon omtales videre i Veileder i verdivurdering.

Det forventes at brukerne av veilederen kjenner sikkerhetsloven med forskrifter og har gjennomført en eller annen form for grunnleggende sikkerhetsopplæring. Veilederen må leses i sammenheng med lov og forskrift, samt NSMs øvrige veiledere og grunnprinsipper.

1.3. Avgrensing

Denne veilederen omhandler i stor grad de teknologiske (fysiske og elektroniske) sikkerhetstiltakene. Veilederen omhandler ikke logiske sikkerhetstiltak. Videre vil veilederen i noen grad også berøre de menneskelige og organisatoriske tiltakene som er avgjørende for at de fysiske og elektroniske sikkerhetstiltakene skal virke etter sin hensikt.

Bestemmelsene i sikkerhetsloven og dens forskrifter vil være et minimumskrav for valg av sikkerhetstiltak mot sikkerhetstruende virksomhet, men i tillegg vil det være andre sektorregelverk som også må tas hensyn til. Denne veilederen vil ikke omfatte særtilpasninger til andre lovverk om hvordan sikkerhetstiltak skal implementeres.

Naturskader blir ikke trukket fram som en selvstendig risikofaktor i veilederen, men må håndteres på lik linje med terror og sabotasje med et tilsvarende skadepotensiale.

Veilederen vil ikke gi virksomhetene konkrete løsningsforslag på etablering av fysiske sikkerhetstiltak. De skjermingsverdige objektenes art, omfang og verdi vil være svært ulike og sikkerhetstiltakene må tilpasses det enkelte objekts særegenheter.

2. Veiledning til bestemmelser om fysisk sikkerhet

Dette kapittelet veileder til aktuelle bestemmelser i virksomhetsikkerhetsforskriften. Krav i virksomhetsikkerhetsforskriften må sees i sammenheng med krav i sikkerhetsloven.

Kapittel 3 (§§ 12-21) er generelle krav til beskyttelse av alle skjermingsverdige verdier, og kan sees på som et minimumskrav for beskyttelse av alle skjermingsverdige verdier. Kapittel 4 (§§ 22 -27) er krav til håndtering og beskyttelse av skjermingsverdig informasjon. Kapittel 6 (§§ 34-48) er ytterligere krav til beskyttelse av informasjon gradert KONFIDENSIELT eller høyere. Kapittel 9 (§§ 58-60) er krav til beskyttelse av skjermingsverdige objekter og infrastruktur.

2.1. Generelt om sikkerhetstiltak (§ 14)

§ 14. Grunnsikringstiltak, påbyggingstiltak og tiltak for skadebegrensning og gjenoppretting

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.

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.

Virksomheten skal ha en plan for å gjenopprette et forsvarlig sikkerhetsnivå.

Grunnsikring er de etablerte, verifiserte og dokumenterte samlede sikkerhetstiltakene som skal beskytte de skjermingsverdige verdiene som er identifisert i en normalsituasjon. Grunnsikringstiltakene opprettes med bakgrunn i virksomhetens risikovurdering basert på det gjeldende trusselbildet. Virksomheten skal teste og verifisere at sikkerhetstiltakene gir et forsvarlig sikkerhetsnivå.

a) Der hvor det etableres fysiske og elektroniske sikkerhetstiltak som barrierer for å hindre ulovlig adgang, skal disse planlegges og settes i system slik at virksomheten kan danne seg et bilde av hvor lang tid det tar å forsere barrierene før en reaksjon er iverksatt og fungerer.
    - Fysiske barrierer opprettes for å kunne hindre eller forsinke adgang til verdier. Fysiske barrierer kan etableres som gjerder, fysisk soneinndeling, skjulte eller synlige hinder.
    - Elektroniske sikkerhetstiltak er tiltak som bruker elektrotekniske utstyr og løsninger for å støtte, supplere eller erstatte fysiske sikkerhetstiltak. Elektroniske barrierer kan være etablering av elektronisk adgangskontroll og TV og videoovervåking (TVO).
    - Menneskelige sikkerhetstiltak er tiltak som påvirker vurderingsevne, kunnskap, adferd og reell evne til å bruke teknologiske sikkerhetstiltak og følge organisatoriske sikkerhetstiltak, og kan oppnås ved å etablere fysisk vakthold og adgangskontroll.

- Organisatoriske barrierer er tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, adferd og/ eller anvendelser av sikkerhetstiltak. Organisatoriske sikkerhetstiltak kan etableres i form av skilting, opplæring og bruk av adgangskort.

b) For å kunne være rustet til å oppdage uønsket sikkerhetstruende aktivitet, bør virksomheten etablere detekterende og varslende sikkerhetstiltak. Effektive detektorer kan være automatisk innbruddsalarmanlegg (AIA) med deteksjon av bevegelse, vibrasjon, varme, (termisk/IR), lys eller lyd. Disse vil kunne gi en tidlig varsling ved brudd på etablerte barrierer.

c) Ved å etablere et oppdatert situasjonsbilde vil virksomheten best mulig kunne iverksette en tilstrekkelig håndtering av en detektert hendelse, og dermed gi mulighet til å reagere på situasjonen. Dette kan gjøres ved å etablere detektorer kombinert TV og videoovervåkning (TVO), som samlet er i stand til å detektere og verifisere en pågående hendelse.

d) For å kunne oppnå tilstrekkelig oppfølging på sikkerhetstruende aktiviteter som er detektert, bør det foreligge en beskrevet reaksjon. Dette kan gjøres gjennom prosedyrer for håndtering av uønskede hendelser, bruk av reaksjonsstyrker, eller andre teknologiske, menneskelige eller organisatoriske tiltak. Reaksjonsstyrker er personer og enheter som tilkalles for å hindre, avverge eller begrense skadene av en uønsket hendelse. Reaksjonsstyrkens oppdrag og bemanning vil avhenge av verdien som skal beskyttes, og kan eksempelvis være egne ansatte, vektere, bevæpnet politi eller militære styrker. Det må være en felles forståelse om forventningen til reaksjonsstyrkens kapasitet og evne til å avverge. Effekten må øves, måles og dokumenteres.

   Tidsregnskap er en metode som gjør virksomhetene i stand til å kunne måle om effekten av sikkerhetstiltakene kan motvirke tap av verdiene som skal beskyttes.
   I et tidsregnskap vurderes tiden det tar fra virksomheten detekterer en sikkerhetstruende hendelse til reaksjonsstyrken er på plass, og tiltak for å stoppe hendelsen har fått en planlagt effekt. Ved å benytte ulike barrierer med dokumentert virkning mot aktuelle trusler, vil sikkerhetstiltakene ha en tidsforsinkende effekt, og et hendelsesforløp vil kunne stoppes.

   T1 > T2 + T3
   T1 = Innbruddstid, tiden det tar å forsere alle etablerte sikkerhetstiltak
   T2 = Deteksjonstid, tiden det tar fra innbruddet starter til det detekteres
   T3 = Responstid, tiden fra deteksjon av innbrudd til reaksjonsstyrke er på plass og starter avverging

   Dersom reaksjonsstyrken greier å motvirke tap av verdiene som skal beskyttes, vil virksomheten kunne påberope seg å ha et positivt tidsregnskap.

e) Ved å kombinere ulike sikkerhetstiltak vil man kunne oppnå en best mulig sikring. Tiltakene skal virke sammen, selvstendig, og ikke motvirke hverandre. De enkelte tiltakene bør fungere uavhengig av hverandre slik at frafall av ett ikke påvirker den totale sikringsevnen. Tiltakene bør understøtte og ha en forsterkende effekt på hverandre. Eksempelvis kan perimetersikring i form av et gjerde støttes av et deteksjonsmiddel som bevegelsessensor og kameraovervåkning.

Påbygningstiltak er tiltak som iverksettes av virksomheten dersom risikoen øker utover det grunnsikringstiltakene ivaretar, og er et ledd i virksomhetens beredskapssystem. Tiltakene skal kunne iverksettes i løpet av kort tid, og det er derfor viktig at virksomheten er kjent med og har øvet på disse. Påbygningstiltak kan etableres ved å forsterke allerede etablerte fysiske, menneskelige, organisatoriske og elektroniske sikkerhetstiltak, eller etablering av helt nye tiltak for å kunne håndtere en identifisert trussel. Dette kan gjøres ved å utvide soner, forsterke perimetersikring, øke patruljering eller bruk av sikringsstyrker. Det skal foreligge en plan for iverksettelse av påbygningstiltak med tydelig ansvarsfordeling. Virksomheten skal legge til rette for samøving med involverte parter.

Når en hendelse oppstår er det viktig å ha gode og innøvde skadebegrensende tiltak på plass. Gjennom grundige forberedelser og trening er det mulig å være i forkant av situasjonen og slik kunne styre utviklingen i ønsket retning. Skadebegrensende tiltak kan være en plan som inkluderer kontroll av tilganger, nødmakulering av skjermingsverdig informasjon, evakuering og flytting av funksjoner.

2.2. Prinsipper ved valg og utforming av sikkerhetstiltak (§ 15)

§ 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.

Når et sikkerhetstiltak kan gripe inn i enkeltpersoners rettssikkerhet eller personvern, skal virksomheten kunne dokumentere hvorfor inngrepet er nødvendig.

Sikkerhetstiltakene skal samlet ha som mål å oppnå forsvarlig sikkerhetsnivå. Tiltakene må virke etter sin hensikt, og fungere sammen for å oppnå samspill mellom mennesker, teknologi og organisasjon. Når en virksomhet skal velge ut og utforme sine sikkerhetstiltak, er det flere prinsipper som må legges til grunn:

a) 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. Tiltak som ikke er hensiktsmessige og praktisk utformet kan av enkelte oppleves som hindringer i hverdagen, og kan dermed resultere i at noen omgår bestemmelser og rutiner. Det er derfor av stor betydning at virksomhetene er bevisste på dette når sikkerhetstiltak og prosedyrer etableres. God sikkerhetskultur i virksomheten er en avgjørende faktor for at de etablerte sikkerhetstiltakene skal fungere etter sin hensikt.

   Ved anskaffelse av eksempelvis et automatisk adgangskontrollanlegg anbefales det at man setter seg inn i ulike produsenters løsninger for å få et anlegg som er tilpasset det faktiske behovet. Det anbefales at anskaffelse alltid gjøres hos en seriøs leverandør som også har et

godt serviceapparat. Det bør ikke overlates til leverandøren alene å komme opp med et forslag til leveranse, men virksomhetens sikkerhetsansvarlig og leverandøren bør gå sammen om å finne de mest hensiktsmessige løsningene.

b) Hensikten med å styre tilgangen til en skjermingsverdig verdi er å hindre at uvedkommende får tilgang til verdien. «Uvedkommende» i denne sammenheng er alle som ikke har behov for tilgang. Det skal ikke gis mer omfattende adgang enn det som er nødvendig for å ivareta en funksjon, eller for å gi tilgang til informasjon.
For internt personell tilsier prinsippet at ikke alle ansatte i virksomheten skal ha adgang til alle områder og kontorer i bedriften, eksempelvis trenger ikke andre enn de som skal drifte en server adgang til serverrommet. For eksterne personer, må man vurdere hvilke områder f.eks. leverandører av varer og tjenester strengt tatt må ha adgang til, samt vurdere om antall leverandører kan reduseres. Se også Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon.

c) 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. Dette innebærer at det skal være flere sikkerhetstiltak for å beskytte en verdi, slik at sikkerheten ikke skal være avhengig av bare ett sikkerhetstiltak.
Bruk av soner for beskyttelse av sikkerhetsgradert informasjon er et eksempel på sikring i dybden. Flere lag med sikkerhetstiltak vil gjøre det vanskeligere og mer tidkrevende for en inntrenger å komme seg forbi sikkerhetstiltakene. I tillegg til den fysiske sikringen er det anbefalt å etablere vakthold, deteksjon, alarmer, adgangskontroll og kontrollrutiner i forbindelse med sonene.

d) 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.

Dersom man for eksempel har en rekke sikkerhetstiltak som alle er avhengige av strøm, vil en aktør enkelt kunne sette disse ut av funksjon ved å kutte strømleveransen.

Virksomheten må iverksette alternative tiltak for å opprettholde funksjonen til sikkerhetstiltaket med redundans. Tiltak kan være av en type som direkte reduserer sannsynligheten for at hendelser rammer et spesifikt objekt eller en infrastruktur. Eksempler på dette er ulike former for barrierer, systemer for tidlig deteksjon av uønskede hendelser, verifikasjonssystemer og ulike former for reaksjon for å stoppe eller redusere omfanget av slike hendelser. Reduksjon av risiko kan også bestå av tiltak som reduserer skadevirkningene dersom en hendelse inntreffer. Dette kan enten være tiltak som baseres på økt redundans eller økt motstandsdyktighet, eller en kombinasjon av slike tiltak. Høy redundans innebærer at det er flere enheter eller delsystemer som bidrar til å opprettholde funksjonen. Dersom noen av enhetene eller delsystemene mister sin funksjon, vil de øvrige kunne fylle funksjonen til den eller de som er falt ut, og dermed forhindre alvorlige konsekvenser.

e) Effekten av sikkerhetstiltakene skal være tilnærmet lik for alle skjermingsverdige verdier med samme sikkerhetsbehov. Med dette menes at virksomhetens skjermingsverdige verdier med likt sikkerhetsbehov kan sikres med ulike tiltak, så fremt de oppnår samme effekt. De ulike inngangene til en skjermingsverdig verdi skal beskyttes like sterkt. Det må være en balanse i tiltakene, og en helhetlig sikring i forhold til aktuell trussel. Dører, vegger og vindu må for eksempel ha samme motstandskraft mot inntrengning. Sikkerheten blir aldri bedre enn det svakeste leddet.
Tidsregnskap kan brukes som en metode for å dokumentere at man har etablert en effektiv sikring mot en definert trusselaktør.

Det skal tas hensyn til enkeltpersoners rettsikkerhet og personvern ved valg av sikkerhetstiltak, og det skal ikke behandles personopplysninger i større grad enn nødvendig ut fra formålet med sikkerhetstiltaket. Der et tiltak kan være inngripende vil det være en plikt til å gjøre en skriftlig nødvendighets- og proporsjonalitetsvurdering.

2.3. Krav om bruk av evaluerte produkter og tjenester (§ 16)

§ 16. Krav om bruk av evaluerte produkter og tjenester

Når en virksomhet velger sikkerhetstiltak, skal den bruke evaluerte produkter og tjenester dersom produktets eller tjenestens funksjon i seg selv er avgjørende for at
a) personer ikke får tilgang til informasjon gradert HEMMELIG eller STRENGT HEMMELIG uten å ha et tjenstlig behov for det
b) personer ikke får tilgang til sikkerhetsgradert informasjon de ikke er autorisert for
c) personer ikke kan overta eller sette ut av drift infrastruktur eller objekter som er klassifisert KRITISK eller MEGET KRITISK.

Evalueringen skal skje gjennom metodisk utvikling og testing av produktet eller tjenesten og være etterprøvbar. Den skal utføres av Nasjonal sikkerhetsmyndighet eller et akkreditert laboratorium utpekt av Nasjonal sikkerhetsmyndighet, gi tillit til produktet eller tjenesten og sikre at produktet eller tjenesten har nødvendig funksjonalitet for å sikre det aktuelle graderingsnivået eller klassifiseringsnivået. Nasjonal sikkerhetsmyndighet kan godkjenne bruk av produkter og tjenester som er evaluert eller sertifisert i andre land.

Der ett sikkerhetstiltak i seg selv er avgjørende for å hindre forholdende beskrevet i punkt a-c, skal dette være evaluert og sertifisert iht. krav fastsatt av NSM.

NSM tar utgangspunkt i ISO sertifiserte produkter og tjenester. Der det ikke eksisterer tilfredsstillende standarder, vil NSM stille eksplisitte krav tilpasset det aktuelle grads- eller klassifiseringsnivå.

2.4. Sertifisering av produkter og tjenester (§ 17)

§ 17 Sertifisering av produkter og tjenester

Kravene til en evaluering etter § 16 kan oppfylles gjennom en sertifisering gitt av Nasjonal sikkerhetsmyndighet eller et akkreditert sertifiseringsorgan utpekt av Nasjonal sikkerhetsmyndighet.

Akkreditering av laboratorier og sertifiseringsorganer skal skje etter ISO- og IEC-standarder.

NSM fastsetter krav til virksomheter som utfører sertifisering og evaluering av produkter og tjenester.

2.5. Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon (§ 22)

§ 22. Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon

Når en virksomhet håndterer en risiko knyttet til ugradert skjermingsverdig informasjon etter § 13, skal tiltakene som et minimum sørge for at informasjonen ikke kan gå tapt, endres eller gjøres utilgjengelig med enkle midler. Dersom risikoen tilsier det, skal informasjonen også beskyttes mot avanserte angrepsmetoder.

Når virksomheten håndterer en risiko knyttet til informasjon gradert BEGRENSET, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom informasjonen ikke med enkle midler kan bli kjent for uautoriserte personer.

Ved valg av sikkerhetstiltak skal virksomheten se behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre.

Begrepet informasjon skal forstås vidt og omfatter fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger. Informasjon er skjermingsverdig dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

Å beskytte informasjon i sikkerhetslovens forstand innebærer å sikre informasjonens konfidensialitet, integritet og tilgjengelighet.

- Med konfidensialitet menes at det har en verdi at informasjonen ikke blir kjent for uvedkommende.
- Med integritet menes at det har en verdi at informasjonen er korrekt.
- Med tilgjengelighet menes at det har en verdi at informasjonen er tilgjengelig ved behov.

All skjermingsverdig informasjon skal beskyttes av integritet- og tilgjengelighetshensyn. Når det gjelder informasjonens konfidensialitet gjelder dette for informasjon gradert BEGRENSET eller høyere.

Fysiske sikkerhetstiltak skal derfor sikre at uvedkomne ikke, med enkle midler, får adgang til rom, bygninger, oppbevaringssteder der skjermingsverdig informasjon håndteres/tilvirkes. Med «enkle midler» forstås at man ikke trenger avansert verktøy, kunnskap eller vilje for å få tilgang til informasjonen.

Hva som er enkle midler vil imidlertid kunne være ulikt fra hva slags type sikkerhetstruende virksomhet man må beskytte seg mot, og må vurderes for de ulike verdiene. Det er virksomhetens risikovurdering som vil være avgjørende for hvilke tiltak som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå.

Dersom identifisert risiko tilsier det, skal skjermingsverdig informasjon også beskyttes mot avanserte angrepsmetoder. Avanserte angrepsmetoder må ses opp mot hvilke trusselaktører, scenarier og metoder som er vurdert som relevante for virksomhetens skjermingsverdige verdier.

2.6. Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere (§ 34)

§ 34. Forsvarlig sikkerhetsnivå for informasjon gradert KONFIDENSIELT eller høyere

Når en virksomhet håndterer en risiko knyttet til sikkerhetsgradert informasjon etter § 13, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom

a) uautoriserte personer ikke kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, uten at virksomheten oppdager det
b) uautoriserte personer ikke kan få tilgang til informasjon gradert HEMMELIG eller høyere, uten at virksomheten oppdager det og kan begrense skadefølgene
c) risikoen for at uautoriserte personer får tilgang til informasjon gradert STRENGT HEMMELIG reduseres til et ubetydelig nivå

Tiltakene for beskyttelse av informasjon gradert KONFIDENSIELT skal være egnet til at virksomheten oppdager at informasjonen er kompromittert. Det vil si at tiltakene gjør det mulig å oppdage om en trusselaktør har fått tak i informasjonen.

For informasjon gradert HEMMELIG skal virksomheten i tillegg til å oppdage at kompromitteringen har skjedd, også være i stand til å begrense skadefølgene. Dette kan oppnås ved ha sikkerhetstiltak som varsler om kompromittering kombinert med ulike reaksjonstiltak. Det kan ytterligere skadebegrenses ved å ha etablert loggføring og sporing av den kompromitterte informasjonen, slik at den graderte informasjonen kan fjernes eller gjøres uvesentlig i ettertid.

For informasjon gradert STRENGT HEMMELIG skal det ikke være mulig for en trusselaktør å få tak i informasjonen. Dette kan oppnås ved at man har en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som til sammen setter virksomheten i stand til å avverge kompromittering, for eksempel ved at destruksjon av dokumenter eller lagringsmedier vil kunne iverksettes.

Hvor omfattende tiltak som må etableres for å ha et forsvarlig sikkerhetsnivå, må besluttes på bakgrunn av virksomhetens risikovurdering.

2.7. Soneinndeling (§ 38)

§ 38. Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere

Virksomheter som har informasjon som er gradert KONFIDENSIELT eller høyere, skal etablere en kontrollert og beskyttet sone for å beskytte den sikkerhetsgraderte informasjonen.

Dersom virksomheten har et område med direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal det etableres en sperret sone rundt området.

Alle virksomheter som tilvirker eller oppbevarer informasjon gradert KONFIDENSIELT eller høyere, plikter å dele inn sine lokaler i fysiske soner, og da alltid en kontrollert og beskyttet sone. Sperret sone skal etableres dersom virksomheten har behov for et område der adgang vil gi direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere.

Hensikten med soneinndelingen er en lagvis beskyttelse der sikkerhetstiltakene øker for hver sone, i samsvar med krav til beskyttelse av informasjonens sikkerhetsgrad.

Sonene skal defineres som henholdsvis kontrollert, beskyttet og sperret – hvorav kontrollert er det minst vitale, og sperret er mest sensitivt.

2.8. Kontrollert sone (§ 39)

§ 39. Kontrollert sone

En kontrollert sone skal være et tydelig avgrenset område der virksomheten skal kunne ha kontroll med personer, kjøretøy og annen aktivitet.

Ved særlig høy risiko skal adgang og ferdsel kontrolleres med en fysisk avgrensning.

Kontrollert sone forstås som en sone som omgir beskyttet og sperret sone. Kontrollert sone skal utformes på en slik måte som gir kontroll over personer, kjøretøy og annen aktivitet i sonen, der sikkerhetstiltak etableres på bakgrunn av virksomhetens risikovurdering.

Dette kan gjøres i form av ulike sikkerhetstiltak. Fysiske og elektroniske sikkerhetstiltak kan være fysiske barrierer (gjerder, porter o.l.), adgangskontroll og skilting. Eksempel på deteksjonstiltak er kameraovervåkning, ulike sensorer og stedlig vakthold.

De valgte kontrolltiltakene må sees i sammenheng med sikkerhetstiltakene i de innenforliggende sonene og utformes slik at man oppnår ønsket effekt i beskyttelsen av informasjonen i de forskjellige sonene. For eksempel, en kontrollert sone uten fysiske barrierer vil stille et høyere krav til sikringen av den innenforliggende beskyttede sonen.

I utformingen av kontrollert sone må det tas høyde for at denne skal kunne fysisk avgrenses for å kunne kontrollere all adgang og ferdsel ved særlig høy risiko.

2.9. Beskyttet sone (§ 40)

§ 40. Beskyttet sone

En beskyttet sone skal ha en fysisk avgrensing der sikkerhetstruende virksomhet skal kunne oppdages.

I en beskyttet sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere lagres i en oppbevaringsenhet godkjent av Nasjonalsikkerhetsmyndighet, eller være under stedlig vakthold.

Personer som skal gis permanent adgang til beskyttet sone skal være sikkerhetsklarert for KONFIDENSIELT. Dersom andre personer skal gis adgang, skal adgangen registreres og personene skal følges av personell med permanent adgang.

Det skal være kontroll med adgangen til en beskyttet sone, og det skal være synlig hvem som har permanent adgang dit.

Beskyttet sone forstås som en sone hvor det behandles eller oppbevares sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, eller hvor det oppbevares sikkerhetsgradert informasjonssystem godkjent for sikkerhetsgradsnivå KONFIDENSIELT eller høyere.

Eksempel på beskyttet sone kan være kontorlokaler der personell har gradert PC eller på annen måte behandler gradert informasjon.

Sonen skal være adskilt fra kontrollert sone med fysiske barrierer og det skal være kontroll med adgangen til sonen. Valg av sikkerhetstiltak må sees i sammenheng med sikkerhetstiltakene i kontrollert sone, og behovet for beskyttelse av en eventuell sperret sone innenfor beskyttet sone.

Oppbevares informasjon gradert KONFIDENSIELT eller høyere i sonen, skal dette gjøres i godkjent oppbevaringsenhet eller være under stedlig vakthold.

Personer som har behov for permanent adgang til sonen skal være sikkerhetsklarert for minimum KONFIDENSIELT.

Det skal være synlig hvem som har adgang til sonen, og det skal være enkelt å kontrollere om personer som befinner seg innenfor sonen har gyldig adgang eller ikke. Dette kan gjøres ved å ha plikt om bæring av synlige adgangskort som viser hvor personen har adgang. Videre må det være tilgjengelig lister med oversikt over personer med permanent adgang samt besøkende med midlertidig adgang. Ikke klarerte personer skal følges av personell med permanent adgang til sonen.

2.10. Sperret sone (§ 41)

§ 41. Sperret sone

Sperret sone skal være tydelig merket med høyeste tillatte graderingsnivå og sikres i samsvar med dette graderingsnivået.

Personer som gis permanent adgang til en sperret sone, skal være sikkerhetsklarert og autorisert for informasjonen i området. Dersom andre personer skal gis adgang, skal adgangen registreres, og personen følges av personell som har permanent adgang.

Det skal være kontroll med adgangen til en sperret sone, og det skal være synlig hvem som har permanent adgang til sonen.

Sperret sone forstås som en sone der adgang kan gi direkte tilgang til sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere.

Typiske sperrede soner kan være operasjonsrom, kommunikasjons- og serverrom, hvelv og arkiv hvor det er behov for å behandle og lagre sikkerhetsgradert informasjon. Dette kan være spesialrom hvor sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere, er åpent eller lett tilgjengelig for den som har adgang.

Ved utforming av sikkerhetstiltak til en sperret sone, skal disse samsvare med kravene for gradsnivået av informasjonen som behandles der, samt det utstyret som er i rommet. Utforming av sikkerhetstiltak for den sperrede sonen må sees i sammenheng med sikkerhetstiltak benyttet i de utenforliggende sonene.

Eksempel: Dersom HEMMELIG informasjon skal behandles eller lagres i sonen, skal hele sonens sikkerhetstiltak utformes på en måte som sikrer at uautoriserte personer ikke kan få adgang til sonen uten at virksomheten oppdager dette, og kan begrense skadefølgene. Jf. § 34 c).

Sperret sone må i tillegg utformes på en måte som hindrer direkte innsyn til skjermingsverdig informasjon fra eksempelvis inngangsdør. Det bør etableres godkjente oppbevaringsmuligheter i sonen for å kunne minimere mengden gradert informasjon som til enhver tid er tilgjengelig.

Sonen skal tydelig merkes med høyeste tillate sikkerhetsgradsnivå.

Permanent adgang skal kun gis til personer som er sikkerhetsklarert og autorisert for informasjonen i sonen. Andre personer kan gis midlertidig adgang, men da kun i følge med person med permanent adgang. Dersom personen skal ha tilgang til informasjon gradert KONFIDENSIELT eller høyere, må de inneha gyldig sikkerhetsklarering og autoriseres for informasjonen det gis tilgang til. Besøksprotokoll etableres for å kunne loggføre besøk av personer uten fast adgang til sonen.

Oversikt over personell med fast adgang til sonen skal være oppdatert og lett tilgjengelig på innsiden av sonen for å sikre at kun autorisert personell får adgang. Denne oversikten bør kun være tilgjengelig for personer med tjenstlig behov for denne informasjonen.

Sikkerhetsgradert informasjon gradert KONFIDENSIELT eller høyere i form av tale, skal skje i sikrede rom og lokaler, slik at informasjonen ikke blir kjent for uautoriserte personer. jf. § 46. Virksomheten skal be Nasjonal sikkerhetsmyndighet vurdere om det skal gjennomføres en teknisk sikkerhetsundersøkelse før et rom eller lokale tas i bruk.

2.11. Fysisk sikring av skjermingsverdige informasjonssystemer (§ 49)

§ 49. Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer

Når en virksomhet håndterer en risiko knyttet til skjermingsverdige informasjonssystemer etter § 13, skal den oppnå et forsvarlig sikkerhetsnivå ved å

a) beskytte data mot uønsket lesing og beskytte tjenester mot uønsket bruk
b) beskytte data mot uønsket modifikasjon og beskytte tjenester mot uønsket modifikasjon og manipulasjon
c) beskytte data mot uønsket sletting og beskytte tjenester mot uønsket reduksjon eller stans
d) identifisere og autentisere brukere som kan påvirke informasjonssystemets funksjon, eller som kan få tilgang til data i systemet, før de gis tilgang til data og tjenester
e) forhindre at falske data og tjenester introduseres i informasjonssystemet
f) registrere bruk, misbruk og forsøk på misbruk av informasjonssystemet, tjenester og data
g) systematisk kontrollere at sikkerhetstiltakene er korrekt implementert og ivaretar g)sikkerheten på en effektiv og hensiktsmessig måte.

Sikkerhetstiltakene skal være tilpasset systemets totale omfang og kompleksitet gjennom hele systemets levetid.

Sikkerhetstiltak som skal virke hurtig, eller som lett kan utløse feil når de utføres manuelt, skal automatiseres så langt det er praktisk mulig

I et skjermingsverdig informasjonssystem vil de fysiske komponentene som bærer sikkerhetsgradert informasjon være å anse som utsatt for kompromittering og manipulasjon på de steder uautoriserte har adgang. Komponentene skal med det beskyttes i henhold til høyeste sikkerhetsgrad for oppbevaring som systemet er godkjent for.

Der hvor skjermingsverdig informasjon er tilgjengelig i et informasjonssystem skal alle fysiske komponenter sikres slik at de møter kravene til beskyttelse av skjermingsverdig informasjon i henhold til § 22.

Informasjonssystemer som behandler sikkerhetsgradert informasjon KONFIDENSIELT eller høyere skal beskytte alle fysiske komponenter i henhold til §§ 38 – 41, der hvor det er fysisk og teknisk mulig å hente ut informasjon.

For informasjonssystemer som behandler informasjon sikkerhetsgradert BEGRENSET eller skjermingsverdig informasjon uten sikkerhetsgrad, bør de samme prinsippene benyttes i utforming og plassering av komponenter så langt dette er mulig.

Sikkerhetstiltakene skal i sum utformes på en måte som hindrer uvedkomne tilgang til skjermingsverdig informasjon eller sikkerhetsgraderte komponenter, samtidig som man opprettholder tilgjengelighet til systemet.

2.12. Fysisk sikring av klassifiserte objekt og infrastruktur (§ 58)

§ 58. Forsvarlig sikkerhetsnivå for klassifiserte objekter og infrastruktur

Når en virksomhet håndterer en risiko knyttet til skjermingsverdige objekter eller infrastruktur etter § 13, er kravet til et forsvarlig sikkerhetsnivå oppnådd dersom virksomheten kan dokumentere at det er foretatt en konkret vurdering av risikoen, og at det er iverksatt nødvendige tiltak for å håndtere den. I vurderingen av om det er iverksatt nødvendige tiltak skal det legges vekt på om sikkerhetstiltakene er egnet til å

a) begrense tap av vesentlige funksjoner ved skadeverk på eller forsøk på å ødelegge objekter eller infrastruktur klassifisert VIKTIG
b) begrense tap av funksjoner ved skadeverk på eller forsøk på å ødelegge objekter eller infrastruktur klassifisert KRITISK
c) avverge tap av funksjoner ved skadeverk på eller forsøk på å ødelegge objekter eller infrastruktur klassifisert MEGET KRITISK
d) avverge en rettsstridig overtakelse av objekter eller infrastruktur klassifisert KRITISK eller MEGET KRITISK

For å kunne oppnå et forsvarlig sikkerhetsnivå, skal virksomheten vurdere å redusere sårbarheten, og dermed risikoen, ved å etablere grunnsikringstiltak og påbygningstiltak.

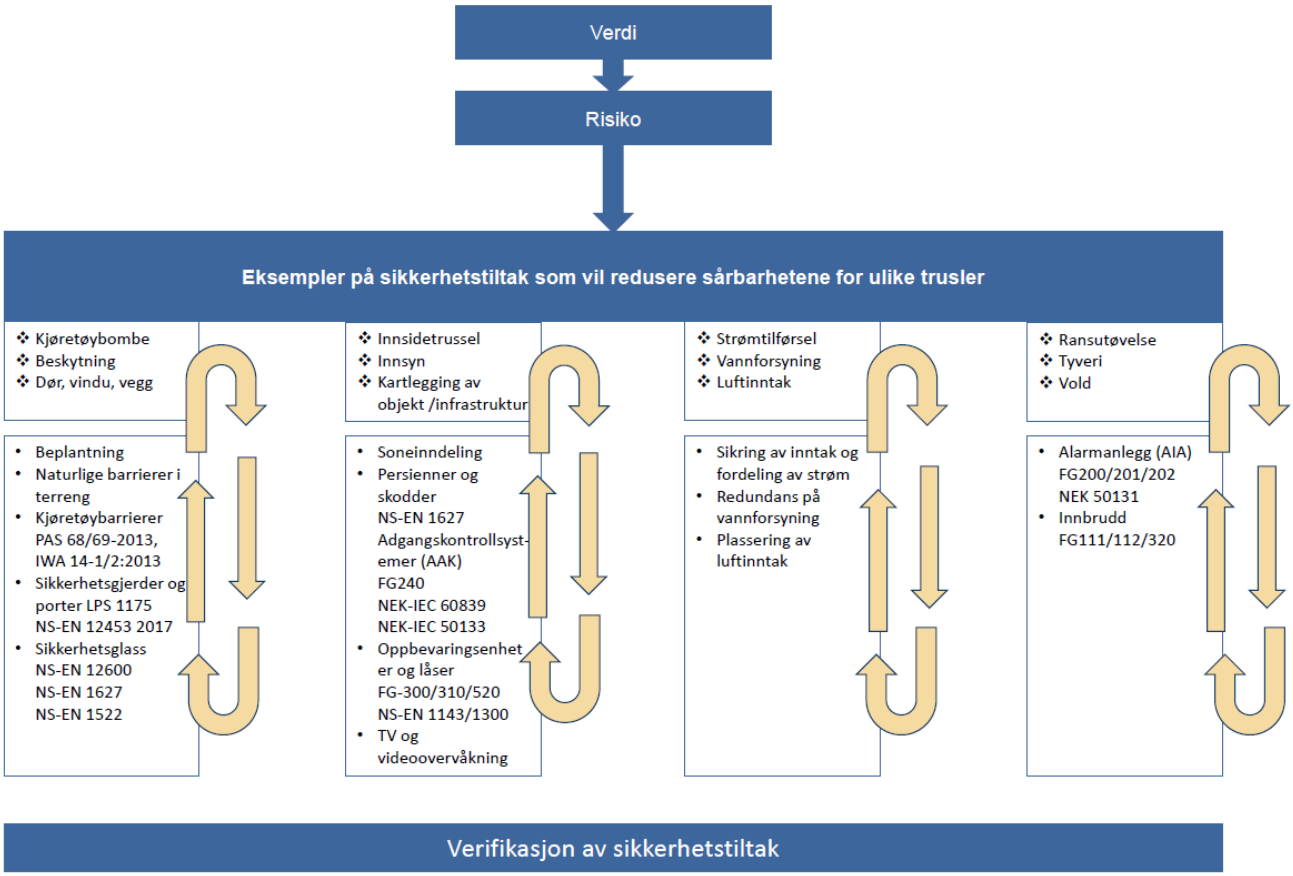
Objekt eller infrastruktur klassifisert VIKTIG skal beskyttes slik at hele eller deler av funksjonen innen rimelig tid kan gjenopprettes til et forsvarlig nivå. Begrepet rimelig tid kan være vanskelig å fastsette, og skadefølgene vil avgjøre hva et akseptabelt nivå på rimelig tid vil være. Skadehåndtering for VIKTIG infrastruktur kan være å ha alternative muligheter til å etablere føringsveier for strøm og data, eller å ha reservedeler tilgjengelig, slik at funksjonen kan gjenopprettes. Dette for å unngå at tjenesten eller funksjonen infrastrukturen representerer, ikke vil påvirke andre klassifiserte grunnleggende nasjonale funksjoner negativt.

Objekt eller infrastruktur klassifisert KRITISK skal beskyttes slik at forsøk på ødeleggelse eller skadeverk begrenses til et nivå som gjør at hele funksjonen raskt kan gjenopprettes til et forsvarlig nivå. Skadebegrensning for funksjoner som er KRITISK, skal håndteres slik at et utfall eller funksjonssvikt ikke får større konsekvenser enn hva som er akseptert. Eksempelvis vil umiddelbar tilgjengelighet på personell, reservedeler o.l. være avgjørende for raskt å kunne gjenopprette funksjonen.

Objekt eller infrastruktur klassifisert MEGET KRITISK skal sikres mot funksjonssvikt og forsøk på ødeleggelse. For å oppnå et forsvarlig sikkerhetsnivå, skal virksomheten kontinuerlig kartlegge kritiske avhengigheter og sikre disse.

For å forhindre rettstridig overtakelse, skal det planlegges og etableres fysiske og elektroniske barrierer med deteksjon og/eller stedlig vakthold med reell evne til å beskytte objekter og infrastruktur klassifisert KRITISK og MEGET KRITISK. Det må være positivt tidsregnskap for fysiske og/-eller elektroniske inntrengning.

3. Eksempel på valg av fysiske sikkerhetstiltak



I figuren over forutsettes det at virksomhetens skjermingsverdige verdier er identifisert og analysert i en risikovurdering.

Sikkerhetstruende virksomhet er tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Eksempel på sikkerhetstiltak mot sikkerhetstruende virksomhet er plassert under de identifiserte sårbarhetene. Figuren over fokuserer i stor grad på de fysiske og elektroniske sikkerhetstiltakene, men for at de skal kunne virke etter sin hensikt så må de menneskelige og organisatoriske sikkerhetstiltakene understøtte disse.

Sikkerhetstiltakene vil kunne fungere mot flere av de identifiserte sårbarhetene, men er i figuren plassert der de synes å ha best effekt.

Ved å planlegge sikkerhetstiltakene i en tidlig fase, når det eksempelvis skal etableres et nytt objekt eller funksjon, vil man ha større forutsetninger for å kunne benytte seg av den fysiske og geografiske plasseringen av verdien for å få ned konstadene på sikkerhetstiltakene, og i tillegg øke sikkerheten.

De beige pilene indikerer virksomhetens plikt til å regelmessig verifisere og teste at sikkerhetstilkatene fortsatt beskytter i henhold til virksomhetens vedtatte sikkerhetsmål.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no