Nasjonal sikkerhetsmyndighet

Veileder for objektsikkerhetsforskriften

En veileder i utvelgelse, klassifisering og beskyttelse av skjermingsverdige objekter

Objektsikkerhetsforskriften stiller krav til utvelgelse, klassifisering og beskyttelse av skjermingsverdige objekter som i henhold til sikkerhetsloven har avgjørende nasjonal betydning. Denne veilederen vil gi en innføring i definisjoner, kriterier og ansvarsforhold for gjennomføring av objektsikkerhetsforskriften.

Versjon 1.2

2014-08-29

UGRADERT

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet er tverrsektoriell fag- og tilsynsmyndighet innenfor forebyggende sikkerhetstjeneste i Norge og forvalter lov om forebyggende sikkerhet av 20 mars 1998. Hensikten med forebyggende sikkerhet er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, primært spionasje, sabotasje og terrorhandlinger. Forebyggende sikkerhetstiltak skal ikke være mer inngripende enn strengt nødvendig, og skal bidra til et robust og sikkert samfunn.

Dato	Versjon	Endringer	Ansvarlig avdeling	Godkjent av
30.09.2011	1.0		FOR	Direktør
20.12.2012	1.1.	Kap 1 -5, 8.	FOR	
28.08.2014	1.2	Definisjoner Kap 1.4, 2.1, 6.1, 6.3, 8 og 8.1	Sikkerhetsstyring	Ass. direktør

Innhold

Innledning 4
Bakgrunn 4
Ordliste og sentrale termer i veilederen 4
Formålet med veilederen 6
Referanser 7
1 Objektsikring 8
1.1 Forebyggende sikkerhet og beredskap 8
1.2 Verdivurdering 8
1.3 Skadevurdering 9
1.4 Risikostyring 10
2 Forskrift om objektsikkerhet 12
2.1 Formålet med regelverket 12
2.2 Virkeområde 12
2.3 Meldeplikten 13
2.4 Øvrige regelverk 13
2.5 Hva kan et skjermingsverdig objekt være? 14
3 Ansvar 17
3.1 Ansvar for utpeking av skjermingsverdige objekter 17
3.2 Objekteiers ansvar 17
3.3 Forholdet mellom sektorregelverk og objektsikkerhetsforskriften 18
3.4 Sektormyndighetenes ansvar 18
3.5 Nasjonal sikkerhetsmyndighets ansvar 19
3.6 Forsvarsdepartementets og Justis- og beredskapsdepartementets særskilte ansvar 21
4 Identifisering og utvelgelse 22
4.1 Utgangspunkt 22
4.2 Ansvar for utpeking av skjermingsverdige objekter 22
4.3 Vurderingskriterier 23
4.4 Ledetråder til vurdering 25
5 Klassifisering av skjermingsverdig objekter 27
5.1 Utgangspunkt 27
5.2 Fastsettelse av klassifiseringsgrad 27
5.3 Registrering og koordinering 28
6 Beskyttelse av skjermingsverdige objekter 30
6.1 Utgangspunkt 30
6.2 Objektsikkerhet og sikkerhetstruende virksomhet 31
6.3 Krav til grunnsikring 32
6.4 Tiltak mot etterretningsvirksomhet 34
6.5 Tilrettelegging for beskyttelse av IKT-infrastruktur 34
6.6 Tiltak mot elektromagnetisk puls og høyfrekvente mikrobølger 35
6.7 Tilrettelegging for bruk av sikringsstyrker 35
6.8 Sikkerhetsklarering og autorisasjon 36
6.9 Rutiner for håndtering av besøk 37
7 Administrative bestemmelser 38
7.1 Kostnadsdekning og dispensasjon fra tiltak 38
7.2 Internkontroll 38
7.3 Tilsyn 38
7.4 Frister 38
7.5 Klageadgang 39
8 Fastsetting av grunnsikringskrav 40
8.1 Forslag til løsning 40
Vedlegg A 46
Lov og forskrift om objektsikkerhet 46
Vedlegg B 47
Skadevurdering i praksis 47
Vedlegg C 56
Ideskjema trusseldefinering 56

Innledning

Bakgrunn

Objektsikkerhetsforskriften handler om utvelgelse, klassifisering og beskyttelse av skjermingsverdige objekter.

Sikkerhetsloven § 3 *— Definisjoner*
Forskrift om objektsikkerhet trådte i kraft 1. januar 2011. Hovedformål med objektsikkerhetsregelverket er å gi en helhetlig og overordnet tilnærming på tvers av samfunnssektorene når det gjelder utvelgelse, beskyttelse og tilsyn med skjermingsverdige objekter. Det forebyggende sikkerhetsarbeidet må imidlertid også ta hensyn til forhold som er spesifikke for den enkelte samfunnssektoren.

Forskrift om objektsikkerhet er hjemlet i Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Sikkerhetslovens formål er å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet eller sikkerhet og andre vitale nasjonale sikkerhetsinteresser, gjennom utøvelse av forebyggende sikkerhetstjeneste. Sikkerhetsloven setter krav til en grunnsikring for informasjon og objekter av spesiell verdi for samfunnet, gjennom blant annet å stille krav til defensive sikkerhetstiltak.

Ordliste og sentrale termer i veilederen

Her følger en liste over sentrale termer og begreper i veileder om objektsikkerhetsforskriften. Ordlisten er ikke uttømmende.

Autorisasjon – Avgjørelse tatt om at en sikkerhetsklarert person gis tilgang til informasjon med angitt sikkerhetsgrad. Autorisasjon involverer bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte (sikkerhetsloven § 3). Til forskjell fra *sikkerhetsklarering*, fastsetter autorisasjon at personen får tilgang til konkret informasjon som vedkommende har tjenstlig behov for.

Beskyttelse – Se *forebyggende sikkerhetstjeneste*.

Elektromagnetisk puls (EMP) – Elektromagnetisk puls er en fortettet strøm av elektromagnetisk stråling, tidligere kjent som ”radiolyn”. Effekten av en EMP kan være alt fra forstyrrelser til ødeleggelser av kretser i elektronisk utstyr.

Forebyggende sikkerhetstjeneste – Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet (ref Lov om forebyggende sikkerhetstjeneste).

Følgeskade – Følgetap, ringvirkning av en skade. Indirekte tap som følge av skade voldt gjennom sikkerhetstruende virksomhet.

Grunnsikring – Sikringstiltak som ivaretar en entitets sikringsbehov ved normaltilstand.

Høyfrekvente mikrobølger (High-power Microwave: HPM) – En variasjon av EMP med retningsdirigert kapasitet.

Kapasitet – evne, herunder ressurser, kunnskap og ferdighet, til å utføre en handling (prNS 5830).

Klassifisering – Skalering som angir den sikkerhetsmessige verdien objektet har i forhold til skadefølger ved *sikkerhetstruende virksomhet* (sikkerhetsloven § 17a).

Kritisk infrastruktur – Anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse (NOU 2006:6 Når sikkerheten er viktigst).

Leveranse – Tjenester og produkter som er utkomme av en virksomhets samfunnsmessige hensikt.

Objekteier – Virksomhet eller person som eier eller på annen måte råder over *skjermingsverdig objekt* (objektsikkerhetsforskriften § 1-2).

Rettssubjekt – Enhver som kan ha rettigheter og plikter.

Rikets selvstendighet og sikkerhet – Grunnleggende norske sikkerhetsinteresser som omfatter stats-, samfunns- og menneskelig sikkerhet, beskyttelse av velferd, miljø og økonomisk trygghet for det norske folk. Norske sikkerhetsinteresser berøres også av den internasjonale rettsorden, menneskerettighetene, demokrati, rettsstatens prinsipper, økonomisk trygghet og livsmiljøet (St.prp. nr. 42 (2003-2004) Den videre moderniseringen av Forsvaret i perioden 2005-2008).

Rikets sikkerhet – se ”*rikets selvstendighet og sikkerhet*”.

Sabotasje – Tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering (sikkerhetsloven § 3).

Sikkerhetsklarering – avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad. (sikkerhetsloven § 3).

Sikkerhetsloven – (LOV 1998-03-20 nr 10:) Lov om forebyggende sikkerhetstjeneste.

Sikkerhetstruende hendelse – Uønsket hendelse tilknyttet *sikkerhetstruende virksomhet*.

Sikkerhetstruende virksomhet – Forberedelse til, forsøk på og gjennomføring av *spionasje*, *sabotasje* eller *terrorisme*, samt medvirkning til slik virksomhet (sikkerhetsloven § 3).

Sikringsstyrker – Bemyndiget personell som kan overvåke eller besitte et objekt for å beskytte dette mot *sikkerhetstruende virksomhet*.

Skjermingsverdig informasjon – Opplysninger unntatt offentlighet og sikkerhetsgradert informasjon.

Skjermingsverdig objekt – Eiendom, områder, bygninger, anlegg, transportmidler, annet materiell, eller deler av slik eiendom som kan skade *rikets selvstendighet og sikkerhet* ved *sikkerhetstruende virksomhet*. Definisjonen kan også være bygninger eller områder hvor personer befinner seg, hvor disse personene for eksempel har en slik funksjon i den nasjonale beslutningsprosessen eller lignende at det vil kunne skade *rikets selvstendighet og sikkerhet* ved bortfall (sikkerhetsloven § 3).

Skadefølge – Effekt og konsekvens for et *skjermingsverdig objekt* ved *sikkerhetstruende virksomhet* (versus følgeskade).

Skadevurdering – Vurdering av de negative konsekvensene for en eller flere verdier dersom en uønskt hendelse skulle inntreffe (prNS 5830). I denne sammenheng skal denne sees opp mot skadefølgene for rikets selvstendighet og sikkerhet og vitale nasjonale sikkerhetsinteresser om et objekt får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtagelse av uvedkommende (sikkerhetsloven § 17a).

Spionasje – Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt (sikkerhetsloven § 3).

Terrorisme – Terrorhandlinger som: ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål (sikkerhetsloven § 3).

Trusselaktør – Personer, forbund eller fremmed makt som tar sikte på å gjennomføre *sikkerhetstruende virksomhet*.

Varslingssystem for digital infrastruktur (VDI) – NSM drifter et nasjonalt sensornettverk for deteksjon av angrep via internett, og analyserer informasjonen fra sensorene. Se også punkt 6.5.

Verdivurdering – En systematisk vurdering av hvilke konsekvenser det kan få dersom ressursene (verdiene) rammes av uønskede tilsiktede handlinger gjennom kartlegging og rangering av virksomhetens verdier, for å identifisere hvilke som er så viktige at de må beskyttes.

Vitale nasjonale sikkerhetsinteresser – se ”*rikets selvstendighet og sikkerhet*”.

Formålet med veilederen

Formålet med denne veilederen er å styrke arbeidet med forebyggende tiltak for skjermingsverdige objekter. Veilederen skal bidra til å sikre en korrekt enhetlig forståelse av objektsikkerhetsregelverket og være et redskap for implementering i sektorene. Gjentagelser i veilederen kan forekomme.

Denne veilederen er å betrakte som et levende dokument og vil bli oppdatert etter hvert som det vinnes erfaring i bruken av regelverket.

Det er gjennomført en oppdatering av veilederen fordi man ønsker å fokusere på den prosessen virksomhetene skal gjennomgå med skadevurderingen av mulig skjermingsverdige objekt. Det er viktig at virksomhetene blir bevisstgjort omkring de objektene som er essensielle for virksomhetens funksjon. Revisjonen av denne veilederen har fokusert på ansvar og pålegg i forbindelse med objektsikkerhetsforskriften, samt søkt å gi ytterligere verktøy for på kunne gjennomføre en skadevurdering av objekter ved virksomhetene.

Referanser

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

Forskrift av 22. oktober 2010 om objektsikkerhet.

Odelstingsproposisjon (Ot.prp.) nr. 49 (1996-97), Om lov om forebyggende sikkerhetstjeneste, Forsvarsdepartementet (1997)

Odelstingsproposisjon (Ot.prp.) nr. 59 (2004-2005), Om lov om forebyggende sikkerhetstjeneste, Forsvarsdepartementet (2005)

Odelstingsproposisjon (Ot.prp.) nr. 21 (2007-2008), Om lov om forebyggende sikkerhetstjeneste, Forsvarsdepartementet (2007)

Norges Offentlige Utredninger (NOU) 2000:24 *Et sårbart samfunn* (Sårbarhetsutvalget) Justis- og Politidepartementet.

Norges Offentlige Utredninger (NOU) 2003:18 *Rikets sikkerhet*, Justis- og Politidepartementet.

Norges Offentlige Utredninger (NOU) 2006:6 *Når sikkerheten er viktigst* (Infrastrukturutvalget) Justis- og Politidepartementet.

Høringsbrev av 3. november 2009 til forskrift om objektsikkerhet (Forsvarsdepartementet).

Direktoratet for Samfunnssikkerhet og Beredskap (DSB) *Nasjonal sårbarhets- og beredskapsrapport: Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner*. (2011)

Forsvarsbygg (2005) Sikringshåndboka. Håndbok i sikring og beskyttelse av eiendom, bygg og anlegg mot terrorhandlinger, spionasje, sabotasje og annen kriminalitet. Forsvarsbygg

Fridheim, H. og Hagen, J. (2007): Beskyttelse av samfunnet (BAS) 5: Sårbarhet i kritiske IKT-systemer, Forsvarets forskningsinstitutt (FFI) 2007.

Fridheim, H. et al. (2001): Beskyttelse av samfunnet (BAS) 3: En sårbar kraftfunksjon, Forsvarets forskningsinstitutt (FFI) 2001.

Hagen, J. et al. (2003): Beskyttelse av samfunnet (BAS) 4: Med fokus på transportsektoren, Forsvarets forskningsinstitutt (FFI) 2003.

Nystuen, K. O. (1998): Beskyttelse av samfunnet (BAS) 2: Sårbarhet i offentlig telekommunikasjon, Forsvarets forskningsinstitutt (FFI) 2001 [gradert BEGRENSET].

Skavland, E.I. og Ø.M. Jakobsen (2000): Objekt- og informasjonssikkerhet: Metode for risiko- og sårbarhetsanalyse, ROSS (NTNU) 2000.

prNS 5830 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger - Terminologi.

prNS 5831 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

1 Objektsikring

1.1 Forebyggende sikkerhet og beredskap

Forebyggende sikkerhet **er tiltak før en hendelse skjer, gjerne for å unngå en hendelse i utgangspunktet.** ***Beredskap*** **er tiltak som gjennomføres i forbindelse med at en hendelse er i utvikling eller har skjedd.**

Sikkerhetsloven § 17b *– Plikt til å beskytte skjermingsverdig objekt*
Forskrift om objektsikkerhet § 3-1 *– generelle krav til beskyttelsen*
prNS 5830 Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi

Sikkerhetstruende hendelser som terrorisme, sabotasje og spionasje er i sin natur trusler som ikke kan forventes å gi et forvarsel. Det er mot denne typen trusler mer hensiktsmessig å fokusere på forebyggende sikkerhet. Objektsikkerhetsforskriften fokuserer på grunnsikringstiltak med muligheter for påbygning ved endret risiko. Det er her viktig å tenke på at grunnsikringstiltak ivaretar sikringsbehovet til det skjermingsverdige objektet ved normaltilstand. En innøvd beredskapsplan bør være en integrert del av grunnsikringstiltakene.

Sikkerhetsloven legger opp til forebyggende sikkerhet med grunnsikringstiltak. Grunnsikringstiltakene skal være balanserte.

Grunnsikringstiltakene vil være de barrierer virksomheten har til å forhindre/avverge/forsinke en angriper – inntil en reaksjonsstyrke er på plass.

1.2 Verdivurdering

En virksomhet plikter å ha oversikt over sine verdier.

Sikkerhetsloven § 2 *– Lovens generelle virkeområde*
Forskrift om objektsikkerhet § 1-1 *– Formål og virkeområde*
Forskrift om objektsikkerhet § 2-1, 7. ledd *– Utpeking av skjermingsverdige objekter*
Kgl.res 27.juni 2003 *– Delegering av myndighet til Forsvarsdepartementet etter sikkerhetsloven §2 tredje ledd.*

Alt forebyggende sikkerhetsarbeid begynner med en verdivurdering der virksomheten kartlegger sine verdier og rangerer disse etter viktighet. Dette er en forutsetning for riktig prioritering av begrensede sikringsresurser, og for utforming av effektive sikringstiltak. I henhold til sikkerhetsloven skal virksomheten gjennom en slik analyse avdekke objekter som er så viktige av hensyn til rikets sikkerhet og vitale nasjonale sikkerhetsinteresser at de må skjermes særskilt mot spionasje, terrorisme og sabotasje.

Verdivurderingen kan gjennomføres som en trinnvis kartlegging av virksomheten.

1. Virksomhetens kritiske leveranser

   Departementene og øvrige sektormyndigheter bør begynne med å kartlegge hvilke leveranser innenfor deres myndighetsområde som er av betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, samt har betydning for kritiske funksjoner for det sivile samfunn. De virksomhetene som forestår denne typen leveranser bør informeres om kritikaliteten staten tillegger deres virksomhet, i den grad dette ikke allerede er gjort kjent gjennom andre prosesser.

Virksomhetene bør begynne med å kartlegge hvilke produkter og tjenester de leverer, og om myndigheten vurderer disse som kritiske. Eventuelt kan virksomheten på selvstendig grunnlag å vurdere om egne leveranser kan ha betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket, betydning for kritiske funksjoner for det sivile samfunn, eller understøtter denne type virksomhet hos en annen virksomhet.

2. Virksomhetens kritiske kapabiliteter

Med utgangspunkt i de identifiserte leveransene må virksomheten deretter identifisere hvilke interne systemer og prosesser virksomheten avhenger av for å kunne utføre de kritiske leveransene. Hva må virksomheten være i stand til å gjøre for å kunne levere sine produkter og tjenester?

3. Verdier

Innenfor rammen av forskrift om objektsikkerhet, vil verdiene som skal kartlegges i hovedsak være fysiske objekter med en funksjon. Dette er de delene av infrastrukturen som er nødvendig for å opprettholde virksomhetens kritiske kapabiliteter, og dermed leveranser.

1.3 Skadevurdering

En god skadevurdering forutsetter at virksomheten på forhånd har kartlagt sine leveranser, kapabiliteter og verdier. Her må virksomheten vurdere konsekvensen (skaden) ved bortfall eller overtakelse av objekter identifisert gjennom verdivurderingen. Skadevurderingen kan gjennomføres som en verdivurdering i omvendt rekkefølge, der en vurderer hvordan bortfall eller urettmessig overtakelse av objektet vil påvirke virksomhetens interne systemer og prosesser, og i forlengelsen av dette virksomhetens leveranser.

Skadevurderingen skal særlig ta hensyn til

a) Betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket,

b) Betydning for kritiske funksjoner for det sivile samfunn,

c) Symbolverdi, og

d) Mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse.

I tillegg må skadevurderingen ta hensyn til akseptabel tidsperiode for funksjonssvikt, mulighet til å gjenopprette funksjonalitet, og hensynet til objektets betydning for andre objekter.

I mange tilfeller kan sektordepartementet selv ha bedre forutsetninger enn objekteier for å vurdere flere av punktene over. Dette fordi vurderingskriteriene til en viss grad legger til grunn strategiske overveielser. Skadevurderingen skal gi departementet et utgangspunkt for å utpeke og klassifisere objekter, der departementet legger til grunn sine egne vurderinger og strategiske og samfunnsmessige prioriteter.

Et objekt er skjermingsverdig når følgen av objektets ødeleggelse, nedsatte funksjonalitet eller rettstridige overtakelse er så omfattende at det kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Et objekt kan dermed være skjermingsverdig på bakgrunn av et eller flere av vurderingskriteriene for skadevurderingen.

1.4 Risikostyring

Sikkerhetsloven med forskrifter stiller krav til at virksomheter som eier skjermingsverdige objekter skal utøve risikostyring. Dette innebærer at virksomhetene skal fastsette og gjennomføre sikkerhetstiltak etter en risikovurdering. Minimumskravene i lov og forskrift er satt på bakgrunn av en overordnet nasjonal risikovurdering. I tillegg plikter virksomheter å utføre risikovurdering med bakgrunn i lokale forhold.

Risikostyring er en kontinuerlig forbedringsprosess. Gjennom objektsikkerhetsforskriften skal samfunnet kartlegge sine verdier i den hensikt å få på plass hensiktsmessige grunnsikringstiltak. Dette skal både avverge muligheten for, samt redusere konsekvensen av sikkerhetstruende hendelser som kan skade rikets sikkerhet. Dette betyr at fagdepartementene kontinuerlig må vurdere sine verdier og sårbarheter og håndtere risikoen. Dette vil kontrolleres ved tilsyn med hjemmel i sikkerhetsloven, eller sektorlovgivning tilpasset sikkerhetslovens funksjonelle krav.

Første trinn i styringssløyfen er, foruten planlegging og organisering; verdivurdering og kartlegging av risikobildet. Dette danner grunnlaget for sikringsanalysen. Denne analysen skal brukes som et grunnlag for planlegging og implementering av sikkerhetstiltak.

I trinn tre utarbeides og implementeres risikoreduserende tiltak. Før nye tiltak kan vurderes må eksisterende sikkerhetsfunksjoner kartlegges. Dette har til hensikt å unngå overlapping og unødvendig bruk av ressurser, samt evaluere om de eksisterende mekanismene er tilfredsstillende. Sikkerhetstiltak, planer og instrukser skal dokumenteres og fremgå av grunnlagsdokument for sikkerhet. Forskriften stiller krav til at sikringstiltakene skal bestå av en kombinasjon av barriere, deteksjon, verifikasjon og reaksjon. Samlet skal de tilfredsstille de funksjonelle kravene til objektets klassifiseringsnivå.

Trinn fire er kontroll og revisjon. Dette skal sikre kontinuitet i sikkerhetsarbeidet med løpende kontroll av de implementerte sikkerhetstiltakene, samt overvåking av trusselbildet. Grunnsikringstiltakene er på plass i utgangspunktet og trusselbildet brukes til å vurdere om ytterligere tiltak skal gjennomføres. Her må virksomheten vurdere om kravene i sikkerhetsloven til skjerming av objektet er tilstrekkelig.

Figur 1: Risikostyringssløyfe.

Styringssløyfen for risikostyring består av fire trinn, der trinn to er en sikringsanalyse.

Objekteiere må bidra til myndighetenes risikostyring gjennom innrapportering av skjermingsverdige objekter. Samtidig skal virksomhetene etablere interne rutiner for risikostyring relatert til objektene. Gradvis bedring i sikkerhetstilstanden gjennom risikostyring forutsetter at styringssløyfen for risikostyring hos sektormyndighetene og objekteier virker sammen.

Sektordepartementene skal ha oversikt over sikkerhetstilstanden i sin sektor. Det er likevel virksomhetens leder som er ansvarlig for sikkerhetstilstanden i egen virksomhet, og har plikt til å følge opp at tilstrekkelig sikkerhetstiltak rundt klassifiserte objekter er implementert og dokumentert. NSM tilbyr råd og veiledning til virksomheter som råder over skjermingsverdig objekt.

2 Forskrift om objektsikkerhet

2.1 Formålet med regelverket

Objektsikkerhetsregelverket skal legge forholdene til rette for bedre sikring av objekter med stor samfunnsmessig betydning, som derfor kan være spionasje-, sabotasje eller terrormål.

Sikkerhetsloven § 1 *– Sikkerhetslovens formål*
Forskrift om objektsikkerhet § 1-1 *– Formål og virkeområde*

Et *"skjermingsverdig objekt"* er eiendom, områder, bygninger, anlegg, transportmidler, annet materiell, eller deler av slik eiendom som kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser dersom de blir utsatt for terror- og sabotasjehandlinger. Dette kan skje ved at objektet kan være et direkte eller indirekte **mål**, eller ved at objektet kan **utnyttes** til slike uønskede handlinger. Objektets skjermingsverdighet vil begrunnes med den funksjon objektet har. Med *"funksjon"* menes produksjon, forsyning, kommunikasjon eller annen rettmessig bruk eller aktivitet tilknyttet objektet.

Objektsikkerhetsarbeidet skal ivareta de forebyggende sikringsbehovene som følger av risikoen for sabotasje og terrorhandlinger. Det stilles krav til objekteierne om å iverksette sikkerhetstiltak for å beskytte objekter av betydning for rikets sikkerhet og vitale nasjonale sikkerhetsinteresser.

Trusselbildet er sammensatt og endrer seg. Truslene kan komme både fra statlige eller ikke-statlige trusselaktører, de kan være av både fysisk, elektronisk og logisk art, og trusselaktørene kan bruke både konvensjonelle og ikke-konvensjonelle midler. Forskriften legger til grunn at «De forebyggende sikkerhetstiltak som utformes mot spionasje, sabotasje og terrorhandlinger må ta utgangspunkt i at mulige trusselaktører er fremmede makter eller internasjonale terrororganisasjoner som har en betydelig kapasitet.» Dimensjonerende trussel vil si det trusselbildet sikringstiltakene skal forebygge, og er uavhengig av dagens trusselbilde.

Sikkerhetslovens formål er å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Dette ivaretas blant annet gjennom utvelgelse og beskyttelse av skjermingsverdige objekter, i tillegg til tilsyn med de utvalgte objektene. Videre skal sikkerhetsloven bidra til å ivareta den enkeltes rettssikkerhet og trygge tilliten til, samt forenkle grunnlaget for, kontroll med forebyggende sikkerhetstjeneste.

2.2 Virkeområde

Sikkerhetsloven gjelder for;

- **forvaltningsorganer i stat og kommune**
- **leverandør av varer eller tjenester i forbindelse med en sikkerhetsgradert anskaffelse**
- **annet rettssubjekt som eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt (etter enkeltvedtak)**

Sikkerhetsloven § 2 *– Lovens generelle virkeområde*

Forskrift om objektsikkerhet § 1-1 *– Formål og virkeområde*
Forskrift om objektsikkerhet § 2-1, 7. ledd *– Utpeking av skjermingsverdige objekter*
Kgl.res 27.juni 2003 *– Delegering av myndighet til Forsvarsdepartementet etter sikkerhetsloven §2 tredje ledd.*

Skjermingsverdige objekter kan befinne seg både i offentlig og privat eie.

Hovedregelen er at bestemmelsene i sikkerhetsloven gjelder for forvaltningsorganer i stat og kommune. Sikkerhetsloven gjelder imidlertid også for ethvert rettssubjekt som er leverandør av varer eller tjenester til et forvaltningsorgan i forbindelse med en sikkerhetsgradert anskaffelse. I tillegg kan det bestemmes at loven helt eller delvis også skal gjelde for ethvert annet rettssubjekt som eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt, eller som av et forvaltningsorgan gis tilgang til sikkerhetsgradert informasjon. Dette skjer gjennom særlig vedtak i Forsvarsdepartementet, som har fått delegert denne fullmakten fra Kongen. I praksis vil dette innebære at det settes i gang en prosess som eventuelt fører frem til et enkeltvedtak om å gjøre loven gjeldende for den aktuelle virksomheten. Forut for dette vil den aktuelle virksomheten ha anledning til å uttale seg. Det vises til videre omtale i punkt 2.4 og 3.3 i denne veiledningen.

2.3 Meldeplikten

Objekteier plikter å melde inn objekt i egen sektor andre virksomheters skjermingsverdige objekt er avhengige av.

Forskrift om objektsikkerhet § 2-1, 5. ledd *– Utpeking av skjermingsverdige objekter*
Eier av skjermingsverdig objekt må informere sektordepartementet om hvilke andre objekter de er avhengig av for å opprettholde sitt eget objekts funksjon. Likeledes skal objekteier som råder over et objekt som en annen virksomhet er avhengig av, melde dette inn til sitt sektordepartement for klassifisering og utpeking som skjermingsverdig objekt. Det pålegges utpekt objekteier å fremlegge dokumenterbar redundans og leveringsdyktighet ovenfor den kritiske virksomheten ved omklassifisering.

Virksomhetene forventes å koordinere informasjon og sikringstiltak på tvers av sektorene for å dekke opp for meldeplikten for skjermingsverdige objekt.

2.4 Øvrige regelverk

Objektsikkerhetsregelverket skal legge til rette for å avdekke tverrsektorielle avhengigheter i normaltilstand.

Sikkerhetsloven § 1 *– Sikkerhetslovens formål*
Sikkerhetsloven kapittel 5. Objektsikkerhet.
Forskrift om objektsikkerhet, kapittel 1 *– Alminnelige bestemmelser*
Forskrift om objektsikkerhet, kapittel 3 *– Beskyttelse av skjermingsverdige objekter*
Kgl.res. 24. august 2012 - *Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker fra Forsvaret og politiet i fred, krise og krig*

Objektsikkerhetsforskriften er et av flere regelverk som ivaretar nasjonal sikkerhet, og skal virke sammen med disse.

Direktiv for uttak og sikring av nøkkelpunkt (Nøkkelpunktdirektivet) – utarbeides av Forsvaret for å sikre personer og objekt som er av betydning for forsvarsevnen ved utløsning av nasjonal krisetilstand eller væpnet konflikt. Dette er lovlige militære mål ved en væpnet

konflikt jf. artikkel 52 i tilleggsprotokoll av 1977 til Genévekonvensjonen av 1949. Disse mulige målene sikres ved hjelp av militære styrker.

Instruks om sikring og beskyttelse av objekter ved bruk av sikringsstyrker fra Forsvaret og politiet i fred, krise og krig - fastsetter bestemmelser for ansvarsforhold og samarbeid om politiets og Forsvarets objektsikring ved bruk av sikringsstyrker. Formålet med objektsikringen er at viktige objekter skal opprettholde sin virksomhet og funksjonalitet i kritiske situasjoner.

Begge disse regelverkene omhandler disponering av sikringsstyrker ved et forvarsel eller for å gjenopprette normaltilstand. De er derfor å regne som beredskapstiltak for utsatte virksomheter. Ikke alle objekt som faller inn under disse planverkene vil være klassifisert som skjermingsverdige objekt. Objektsikkerhetsforskriften stiller imidlertidig krav til at det skal kunne tilrettelegges for at sikringsstyrker skal kunne øve på objektet. Det er derfor en naturlig konsekvens at der det er hensiktsmessig harmoniseres disse planverkene opp mot skjermingsverdige objekt.

Sektorregelverk – det foreligger spesifikke sikringskrav for en rekke virksomheter underlagt særlige sektorregelverk. Objekteier må, uavhengig av eget sektorregelverk, tilfredsstille sikkerhetslovens funksjonelle krav, og har uansett meldeplikt i forhold til objektsikkerhetsforskriften.

2.5 Hva kan et skjermingsverdig objekt være?

Sikkerhetsloven § 3-12 *– Definisjoner*
Sikkerhetsloven § 17 *– Utvelgelse av skjermingsverdige objekter*
Sikkerhetsloven § 17, 2. ledd *– Utvelgelse av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 2-1, 5. ledd *– Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 2-2, 2. ledd *– Klassifisering*
Forskrift om objektsikkerhet § 2-2, 3. ledd *– Klassifisering*
Forskrift om objektsikkerhet § 2-4, 4. ledd *– Registrering og koordinering*

Hva har lovgiver ment med begrepene ”*rikets selvstendighet og sikkerhet”* og andre ”*vitale nasjonale sikkerhetsinteresser”* som er sentrale i forståelsen av skjermingsverdige objekt?[1]

Det går frem av Ot.prp. nr. 49 (1996-1997) at forsvar av rikets territorium og vår alliansetilknytning tradisjonelt har utgjort kjernen i begrepet ”rikets sikkerhet”, men at også andre forhold vil omfattes av begrepet. Lovgiver fant det nødvendig å inkludere andre vitale nasjonale sikkerhetsinteresser i et utvidet sikkerhetsbegrep.

> *”Begrepet ”vitale nasjonale sikkerhetsinteresser” ble innført i sikkerhetsloven for å gi den et virkeområde som omfatter samtlige felter innenfor rikets totale sikkerhetsbehov.” (…) ”For det første må det fremheves at opplysningene må være knyttet til rikets sikkerhetsmessige interesser. I ordet ”vitale” ligger videre en forutsetning om at det må dreie seg om helt essensielle og samfunnsviktige sikkerhetsinteresser(…)”*

Videre legges det til grunn at begrepet ”rikets sikkerhet” er en rettslig standard, som innebærer at meningsinnholdet vil avhenge av samfunnsutviklingen.

> *”Begrepet må derfor til enhver tid vurderes og defineres av overordnede politiske myndigheter. Terskelen for i medhold av denne loven å anse noe for å true slike interesser, vil være høy.”*

[1] Hva som omfattes av begrepet ”rikets sikkerhet” har vært drøftet ved flere anledninger over tid. Det vises her særlig til lovforarbeidet til sikkerhetsloven, straffelovkommisjonens utredning fra 2003 og Infrastrukturutvalgets utredning NOU 2006:6 ”Når sikkerheten er viktigst”.

I 2003 la Straffelovkommisjonen til grunn at nasjonal handlefrihet og integritet også må omfattes av begrepet "rikets sikkerhet" [2]. Kommisjonen viser til at andre grunnleggende nasjonale interesser er vann-, mat- og energiforsyning, helseberedskap, (tele)kommunikasjon, samferdsel, bank- og pengevesen.

Infrastrukturutvalget mente at det var viktig at terskelen for å anse noe for å true «rikets sikkerhet» og «vitale nasjonale interesser» skal være høy[3].

I Infrastrukturutvalgets utredning favnet begrepene «rikets sikkerhet» og «vitale nasjonale interesser» sikringen av landets kritiske infrastruktur og kritiske samfunnsfunksjoner.

> "*Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse."*

Til sammen er dette med på å understøtte rikets sikkerhet og landets vitale nasjonale interesser. Infrastrukturutvalget la til grunn at dette var de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse er å anse som kritisk infrastruktur.

Infrastrukturutvalget utarbeidet en oversikt over kritiske infrastrukturer og kritiske samfunnsfunksjoner (figur 1). Utvalget vurderte ikke eksplisitt de kritiske samfunnsfunksjonene som står i kursiv[4].

Kritisk infrastruktur	**Kritiske samfunnsfunksjoner**
Elektrisk kraft Elektronisk kommunikasjon Vann og avløp Transport Olje og gass Satellittbasert infrastruktur	Bank og finans Matforsyning Helse-, sosial- og trygdetjenester Politi Nød- og redningstjeneste Krisetjeneste
	Storting og Regjering *Domstolene* *Forsvaret* *Miljøovervåkning* *Renovasjon*

Figur 2: Kritiske infrastrukturer og kritiske samfunnsfunksjoner.

Direktoratet for samfunnssikkerhet og beredskap (DSB) har også utarbeidet en liste med kritiske samfunnsfunksjoner og kritiske allmenne innsatsfaktorer[5].

Det kan tas utgangspunkt i disse oversikter for å identifisere skjermingsverdige objekter. I tillegg vises det til BAS-studiene fra Forsvarets forskningsinstitutt (FFI) som er mer sektororienterte[6].

[2] NOU 2003:18 "Rikets sikkerhet". Nasjonal handlefrihet og integritet kan i følge kommisjonen brytes ned til underpunkter, hvor handlefrihet på følgende områder er vesentlig: Konstitusjonelt, juridisk, sikkerhetspolitisk, økonomisk og finansielt, innenriks- og utenrikspolitisk handlefrihet i tillegg til territoriell integritet.

[3] NOU 2006:6 *Når sikkerheten er viktigst.*

[4] NSM viser særlig til kapittel 10 og 11 i Infrastrukturutvalgets utredning om kritisk infrastruktur og kritiske samfunnsfunksjoner.

[5] Direktoratet for Samfunnssikkerhet og Beredskap (DSB) *Nasjonal sårbarhets- og beredskapsrapport: Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner* (2011).

Gjensidig avhengighet preger mange samfunnskritiske funksjoner og kritiske infrastrukturer. Det gjelder spesielt avhengigheter mellom elektronisk kommunikasjon og kraftforsyning. Mange kritiske samfunnsfunksjoner vil i stor grad være avhengig av eksterne kritiske infrastrukturer for opprettholdelse av funksjonsdyktighet.

[6] Se referanselisten punkt 1.3.

3 Ansvar

3.1 Ansvar for utpeking av skjermingsverdige objekter

Objekteier har plikt til å foreslå hvilke objekter som kan være skjermingsverdige.

Sektordepartement plikter å foreta utpeking og tilsyn med sikkerhetstilstanden.

Sikkerhetsloven § 17 *– Utvelgelse av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 2-1 *– Utpeking av skjermingsverdige objekter*

Sikkerhetsloven har allerede bestemmelser for hvilke objekter som er skjermingsverdige, og hvordan disse skal sikres. Gjennom forskrift om objektsikkerhet gjøres både fagdepartementene og eiere av skjermingsverdig objekt, ansvarlig for at statens verdier skal kartlegges og lovpålagt grunnsikring etableres. Sektormyndigheten har det overordnede ansvaret for utpeking og klassifisering av objekter, mens objekteier står ansvarlig for innrapportering og det praktiske sikringsarbeidet. Objekteier plikter overfor departementet å foreslå hvilke objekter som er skjermingsverdige.

3.2 Objekteiers ansvar

Objekteier plikter å beskytte objektet med sikkerhetstiltak.

Et objekt kan være skjermingsverdig selv om dette ikke er formalisert ved utpeking av sektordepartement. Manglende innrapportering fritar ikke objekteier for ansvar.

Sikkerhetsloven § 3, nr 14 *– Definisjoner*
Sikkerhetsloven § 17, 1. ledd *— Utvelgelse av skjermingsverdige objekter*
Sikkerhetsloven § 17 b 3. ledd *— Plikt til å beskytte skjermingsverdige objekt*
Forskrift om objektsikkerhet § 2-1, 1. ledd *– Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 3-2, 1. ledd *– Tiltak mot etterretningsaktivitet*
Forskrift om objektsikkerhet § 3-3 *– Tilretteleggelse for beskyttelse av IKT-infrastruktur*
Forskrift om sikkerhetsadministrasjon

Virksomhet eller person som eier eller på annen måte råder over skjermingsverdige objekt er å betrakte som objekteiere. Når det er andre enn eieren som råder over objektet, er dette vedkommende som er å anse som objekteier. Eksempelvis er ikke Statsbygg å betrakte som objekteier, men den virksomheten som leier lokaler av Statsbygg og som har en funksjon tilknyttet objektet. Forskrift om objektsikkerhet er en presisering av bestemmelsene i sikkerhetsloven. Dette betyr at objekteier hele tiden har hatt et ansvar for å beskytte objekter som oppfyller sikkerhetslovens kriterier for skjerming, og skal ikke kunne undra seg dette ansvaret gjennom manglende innrapportering.

Gjennom forskriften pålegges objekteier å identifisere mulige skjermingsverdige objekter. Dette gjøres gjennom en dokumentert skadevurdering til sektorens fagdepartement. Objekteier plikter å beskytte objektet med sikkerhetstiltak i forhold til klassifiseringsgrad på objektet. Ved fastsetting av sikkerhetstiltak vises det til krav om internrevisjon, i henhold til forskrift om sikkerhetsadministrasjon.

Sikkerhetstiltakene skal være utformet slik at de kan forsterkes hurtig ved økt trusselnivå. Objekteier skal også legge til rette for at sikringsstyrker skal kunne forberede, øve og gjennomføre tiltak på og ved objektet for å beskytte dette. Det understrekes at beredskapstiltak ikke kan erstatte grunnsikringstiltak.

Et skjermingsverdig objekt skal være beskyttet mot informasjonsinnhenting som kan ha til hensikt å forberede sabotasje eller terrorhandling mot objektet. Med hjemmel i sikkerhetslovens kapittel 4 skal virksomhetene vurdere sikkerhetsgradering av informasjon om objektet, som et naturlig sikkerhetstiltak mot denne typen informasjonsinnhenting.

Dersom objekteierne mener sikkerhetsklarering for personell med permanent tilgang til objektet er et hensiktsmessig barrieretiltak, må dette begrunnes ovenfor det aktuelle fagdepartement.

3.3 Forholdet mellom sektorregelverk og objektsikkerhetsforskriften

Mange sektorregelverk har bestemmelser om sikring av objekter. Sikring mot uønskede hendelser etter sikkerhetsloven må sees i sammenheng med de tiltak som er nedfelt i sektorlovgivning (særlover). Sikkerhetstiltakene må tilpasses den enkelte sektor.

Sektorlovgivningen, der den gir bestemmelser om konkrete sikkerhetstiltak mot tilsiktede hendelser, skal derfor legges til grunn ved implementering av forebyggende tiltak. Objektsikkerhetsbestemmelsene i sikkerhetsloven legges til grunn der sektorlovgivningen ikke tilfredsstiller sikkerhetslovens norm for beskyttelse av skjermingsverdige objekter. Ytterligere sikringstiltak som kan være formålstjenlig må vurderes implementert.

Dette reiser spørsmålet om hvilket regelverk som skal gå foran dersom regelverkene ikke harmoniserer eller det oppstår motstrid mellom dem. Det følger av forarbeidene til sikkerhetsloven at sikkerhetslovens bestemmelser om objektsikkerhet er å anse som generelle bestemmelser i forhold til annen lovgivning om sikring av spesielle typer objekter.

På områder der det er gitt spesielle bestemmelser i annen lovgivning skal sikkerhetsloven likevel komme til anvendelse, dersom bestemmelser i andre regelverk ikke i tilstrekkelig grad ivaretar de funksjonelle kravene i sikkerhetslovens kapittel 5 og objektsikkerhetsforskriften. Sektormyndighetene har et ansvar for å sørge for at de funksjonelle kravene er i samsvar med sikkerhetslovens krav.

3.4 Sektormyndighetenes ansvar

Hvert enkelt departement skal:

- **utpeke skjermingsverdige objekter og fastsette klassifiseringsgrad innenfor sitt fagområde**
- **føre register over skjermingsverdige objekter i egen sektor**
- **melde alle skjermingsverdige objekter til NSM.**

Sikkerhetsloven § 17, 1. ledd *– Utvelgelse av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 1-3, 1. ledd *– Forholdet til sektorlovgivning og sektormyndigheter*
Forskrift om objektsikkerhet § 2-1, 1. ledd *– Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 2-1, 7. ledd *– Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 2-2, 1. ledd – *Klassifisering*
Forskrift om objektsikkerhet § 2-4, 1. ledd *– Registrering og koordinering*
Forskrift om objektsikkerhet § 4-3, 2. ledd *– Tilsyn og påleggskompetanse*

Lovgiver har lagt stor vekt på sektorprinsippet. Departementene skal ha gjennomført en prosess for utvelgelse av skjermingsverdige objekt overfor mulige objekteiere. Ettersom risikobildet endrer seg og avhengigheter avdekkes er det viktig at departementene etablerer

rutiner for å avdekke skjermingsverdige objekter gjennom kontinuerlig revisjon av sine sektorer. Ikke-statlige objekteiere som ligger utenfor departementenes styringslinje må følges opp spesielt.

Objekteier er forpliktet til å utarbeide en skadevurdering som grunnlag for departementets vurdering i forhold til utvelgelse. Deretter skal departementet lage en egen vurdering knyttet til klassifisering. Denne vil være basert på informasjon fra skadevurderingen knyttet til utvelgelsen, i tillegg til andre relevante opplysninger. Dette skal resultere i to ulike ettersporbare vurderinger.

Tilsynsorgan for sektoren kan foreslå skjermingsverdige objekter uavhengig av objekteiers forslag. Det kan være uenighet mellom sektortilsyn og objekteier om et objekts betydning. Der objekteier ikke har identifisert det samme skjermingsverdige objektet som tilsynsmyndigheten, kan departementet be objekteier om at det utarbeides en skadevurdering for det aktuelle objekt. Departementet må gjennomgå skadevurderingene og fatte en beslutning om objektets status. NSM tilbyr veiledning i denne prosessen, men endelig ansvar for utpeking av objekter ligger hos departementene.

Der flere objekteiere er avhengig av felles infrastruktur (som for eksempel infrastruktur i departementsfellesskapet), skal ansvaret for oppfølging løftes opp på et overordnet nivå eller reguleres avtalemessig.

I de tilfelle der det er uklart hvilket departement et objekt hører inn under, må departementene samordne seg. Der NSM registrerer at initiativ til dette ikke er tatt, vil NSM søke å igangsette en slik prosess i forhold til aktuelle departementer.

Departementenes ansvar omfatter å velge ut, klassifisere og føre register over de skjermingsverdige objekt som ligger inn under deres fagområde, inklusive underliggende virksomheter. Departementene skal i samarbeid med NSM ivareta nødvendig koordinering slik at hensynet til tverrsektoriell avhengighet blir ivaretatt.

Alle skjermingsverdige objekter skal rapporteres til NSM, men det er departementene som skal sitte på detaljoversikten i sin sektor. Det er departementenes ansvar å foreta en avveining om hvorvidt det skal kreves sikkerhetsklarering for permanent adgang til objekter klassifisert som KRITISK og MEGET KRITISK.

Departementene har beslutningskompetanse vedrørende sikkerhetsprosedyrer for besøk av representanter fra fremmede stater, internasjonale organisasjoner og utenlandske rettssubjekter.

Der en virksomhet med et skjermingsverdig objekt ikke er underlagt sikkerhetsloven, er det departementenes oppgave å initiere forslag om virksomheten som objekteier skal legges under loven. Forslag om å underlegge en virksomhet under sikkerhetsloven fremlegges Forsvarsdepartementet for avgjørelse.

3.5 Nasjonal sikkerhetsmyndighets ansvar

Sikkerhetsloven kapittel 3. Nasjonal sikkerhetsmyndighet
Sikkerhetsloven § 12 *– Plikt til å beskytte sikkerhetsgradert informasjon*
Sikkerhetsloven § 20, 1. ledd *– Gjennomføring av personkontroll*
Forskrift om objektsikkerhet § 2-1, 3. ledd *– Utpeking av skjermingsverdige objekter*

***Forskrift om objektsikkerhet § 2-4, 2. ledd** – Registrering og koordinering*
***Forskrift om objektsikkerhet § 2-4, 4. ledd** – Registrering og koordinering*
***Forskrift om objektsikkerhet § 3-1, 7. ledd** – Generelle krav til beskyttelsen*
***Forskrift om objektsikkerhet § 3-3, 7. ledd** – Tilrettelegging for beskyttelse av IKT-infrastruktur*
***Forskrift om objektsikkerhet § 3-6, 3. ledd** – Sikkerhetsklarering og autorisasjon*
***Forskrift om objektsikkerhet § 4-3, 2. ledd** – Tilsyn og påleggskompetanse*

Nasjonal sikkerhetsmyndighets hovedoppgave er å koordinere de forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden. Dette er nærmere beskrevet i et eget kapittel i sikkerhetsloven.

NSM har en overordnet rolle i forhold til oppfølging av objektsikkerhetsbestemmelsene og skal bidra til at det er en helhetlig tilnærming på tvers av samfunnssektorene når det gjelder *utvelgelse*, *beskyttelse* og *tilsyn* med skjermingsverdige objekter.

NSM skal i samarbeid med fagdepartementene sørge for nødvendig koordinering for å ivareta hensynet til tverrsektorielle avhengigheter mellom objekter. Dette innebærer blant annet å kunne avdekke gjensidige avhengigheter som ikke nødvendigvis vil la seg fange opp i en sektoriell vurdering.

Med utgangspunkt i dette, vil NSM gjennomføre tiltak for å kartlegge tverrsektorielle avhengigheter mellom skjermingsverdige objekter.

NSM har rett til å foreslå objekter ovenfor departementene. Dette vil for eksempel kunne skje der det er avdekket gjensidige avhengigheter mellom objekter, hvor det er forvaltningsområder der det ikke eksisterer tilsynsorgan for et skjermingsverdig objekt, eller for sektorer der det ikke er pekt ut noen objekter.

NSM vil føre en oversikt over alle skjermingsverdige objekter med klassifiseringsgrad av hensyn til NSMs koordineringsrolle. Det er følgelig av betydning at de opplysninger som innrapporteres er så relevante og presise som mulig. Der hvor det foreligger endringer i det skjermingsverdige objektet knyttet til klassifisering meldes dette inn fra departementene til NSM. Slike endringer kan for eksempel være eierskifter, organisasjonsendringer, etablering av redundans og lignende.

NSM har utarbeidet et eget innmeldingsskjema for skjermingsverdige objekt til bruk for departementene[7].

NSM skal føre tilsyn med at utvelgelse og klassifisering av skjermingsverdige objekter skjer etter lovens intensjon. Gjennom denne aktiviteten skal NSM bidra til at objektsikkerhetsforskriften praktiseres på grunnlag av de samme kriterier av sektormyndighetene.

NSM skal ha oversikt over hvilke skjermingsverdige objekter det kreves sikkerhetsklarering for å få permanent adgang til. Der det stilles krav om sikkerhetsklarering for å ha permanent tilgang til et skjermingsverdig objekt, skal NSM informeres om hvilke skjermingsverdig objekt det dreier seg om blant annet av hensyn til å etablere en mest mulig enhetlig praksis.

NSM drifter et nasjonalt sensornettverk på internett i forhold til samfunnskritisk infrastruktur og informasjon (ref. VDI i ordlisten). Der tilknytning til internett utgjør en sårbarhet for sikkerheten til et skjermingsverdig objekt, kan fagdepartementet i samråd med objekteier bestemme at det skal søkes NSM om tilknytning til et sentralt system for varsling av

[7] Vil sendes departementene fra NSM.

koordinerte angrep via internett. NSM vil gi nærmere retningslinjer om hvordan tilknytning kan settes opp og forvaltes.

3.6 Forsvarsdepartementets og Justis- og beredskapsdepartementets særskilte ansvar

Sikkerhetsloven § 2, 3. ledd *– Definisjoner*
Forskrift om objektsikkerhet § 2-1, 6. ledd *– Utpeking av skjermingsverdige objekter*
Kgl.res 27.juni 2003 *– Delegering av myndighet til Forsvarsdepartementet etter sikkerhetsloven §2 tredje ledd.*
Kr.pr.reg.res av 4. juli 2003 *– Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.*

Det overordnede ansvaret for forebyggende sikkerhet i henhold til sikkerhetsloven er delt mellom Forsvarsdepartementet og Justis- og beredskapsdepartementet, for henholdsvis militær og sivil sektor. Departementenes utøvende ansvar ivaretas av NSM. Forsvarsdepartementet er regelverksforvalter for sikkerhetsloven og har også det administrative ansvaret for NSM.

Forsvarsdepartementet er delegert fullmakt til å bestemme hvorvidt sikkerhetsloven skal gjøres gjeldende for et rettssubjekt som ikke er underlagt sikkerhetsloven. Dette gjøres ved at det settes i gang en prosess som eventuelt fører frem til et enkeltvedtak om å gjøre sikkerhetsloven gjeldende for den aktuelle virksomheten. Forut for dette vil alltid den aktuelle virksomheten ha anledning til å uttale seg.

4 Identifisering og utvelgelse

4.1 Utgangspunkt

Hvilke objekter som har størst sikkerhetsmessig verdi må identifiseres. Utvelgelsen skal være basert på en skadevurdering.

Sikkerhetsloven § 17 *— Utvelgelse av skjermingsverdige objekter*
Sikkerhetsloven § 17 b 3. ledd *— Plikt til å beskytte skjermingsverdige objekt*
Forskrift om objektsikkerhet § 2-1 – *Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 3-1 *– Generelle krav til beskyttelsen*

Det er et grunnleggende prinsipp for alt forebyggende sikkerhetsarbeid at man definerer hva som har sikkerhetsmessig verdi, det vil si at man identifiserer og klassifiserer det som er beskyttelsesverdig ut fra:

- en vurdering av hva som kan tenkes å bli rammet av sikkerhetstruende virksomhet
- en vurdering av viktigheten av å unngå at sikkerhetstruende virksomhet oppnår sitt formål (uttrykt ved skadeverdi).

Potensielle skadefølger av sikkerhetstruende virksomhet mot skjermingsverdige objekter må være omfattende i et nasjonalt perspektiv. Funksjonssvikt eller ødeleggelse vil kunne eksempelvis utløse nasjonal katastrofe som innebærer fare for mange menneskers liv, eller ramme virksomheters evne til å gjennomføre grunnleggende samfunnsoppgaver.

Ikke alle objekter vil være like viktige å beskytte. Jo større samfunnsmessig konsekvens det får dersom et objekt ødelegges, jo større sikkerhetsmessig verdi har objektet. Det er derfor nødvendig å utpeke hvilke objekter som skal være skjermingsverdige og klassifisere dem etter sikkerhetsloven § 17 a. Dette vil bidra til mest mulig korrekt tilpasset ressursbruk og minst mulig inngripen overfor eier, ansatt, bruker og andre med tilknytning til objektet. Målet med verdivurderingen er at objektet får en tilstrekkelig og nødvendig beskyttelse ut ifra den konkrete skadevurderingen.

Alt av eiendom, områder, bygninger, anlegg, transportmidler, annet materiell, eller deler av slik eiendom som er av avgjørende betydning for opprettholdelse av funksjonalitet i kritiske infrastrukturer og kritiske samfunnsfunksjoner; skal vurderes i forhold til om de skal beskyttes som skjermingsverdige objekter i henhold til dette regelverket.

4.2 Ansvar for utpeking av skjermingsverdige objekter

Hvert enkelt departement skal utpeke skjermingsverdige objekter innen sitt myndighetsområde.

Objekteier plikter å foreslå mulig skjermingsverdige objekt overfor sitt departement.

Sikkerhetsloven § 17 *– Utvelgelse av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 2-1 *– Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 1-3 *– Forholdet til sektorlovgivning og sektormyndigheter*

I samsvar med sektorprinsippet er vedkommende fagdepartement ansvarlig for å utpeke og klassifisere skjermingsverdige objekter. Det forutsettes imidlertid at den som eier eller råder

over objekter skal aktivt ta del i identifisering og klassifisering av egne skjermingsverdige objekter. Objekteiere har plikt til å foreslå hvilke objekter som er skjermingsverdige overfor departementet.

Et forslag til prosesstart kan være nedsette et utvalg eller en arbeidsgruppe som favner virksomheten bredt for å ikke utelate nominering av mulige skjermingsverdige objekter. Med utgangspunkt i definisjonen av skjermingsverdige objekt (i kapitel 2.3), vil man med kjennskap til virksomheten kunne gjøre en vurdering knyttet til hvilke objekter som vil kunne falle inn under denne kategorien. Det vil også være andre tilnærminger enn denne foreslåtte som kan her kan være hensiktsmessig.

Når det antas at et objekt er skjermingsverdig, skal det utarbeides en skadevurdering for objektet. Denne analysen er en konkret verdivurdering av hvilke skadefølger det vil ha for rikets selvstendighet og sikkerhet og vitale nasjonale sikkerhetsinteresser, dersom et skjermingsverdig objekt skulle bli utsatt for en terror- eller sabotasjehandling.

Virksomheten skal overfor vedkommende fagdepartement levere en dokumentert skadevurdering over hvilke objekter som kan være skjermingsverdige. Skadevurderingen bør inneholde en vurdering av skadefølgene for egen virksomhet og for samfunnet generelt.

Der det finnes tilsynsorgan for sektoren, kan disse foreslå skjermingsverdige objekter uavhengig av objekteiers forslag. Som tilsynsorganer i denne kontekst, mener vi slike som har et særlig ansvar for sikkerhets- og beredskapsarbeid innen den aktuelle sektoren. NSM kan også foreslå skjermingsverdige objekter for departementene. NSM vil blant annet kunne ta initiativ til dette, der hvor det er tvil om hvilken sektor et objekt tilhører.

4.3 Vurderingskriterier

Det skal være en høy terskel for utvelgelse av skjermingsverdige objekter. Det må dreie seg om objekter som etter en skadevurdering må anses helt essensielle for samfunnsviktige interesser.

Sikkerhetsloven § 17 — *Utvelgelse av skjermingsverdige objekter*
Sikkerhetsloven § 17 b 3. ledd — *Plikt til å beskytte skjermingsverdige objekt*
Forskrift om objektsikkerhet § 2-1 – *Utpeking av skjermingsverdige objekter*
Forskrift om objektsikkerhet § 3-1 – *Generelle krav til beskyttelsen*

Identifisering av skjermingsverdig objekt skal skje på grunnlag av en skadevurdering, der det særlig skal tas hensyn til objektets:

a) **betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket,**

b) **betydning for kritiske funksjoner for det sivile samfunn,**

c) **symbolverdi, og**

d) **mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse**

I skadevurderingen skal det tas hensyn til akseptabel tidsperiode for funksjonssvikt, mulighet til å gjenopprette funksjonalitet, og hensynet til objektets betydning for andre objekter.

Departementene må konkret vurdere hva som er akseptabel tidsperiode for funksjonssvikt og hvilke muligheter det er for å gjenopprette funksjonalitet for hvert skjermingsverdig objekt.

Potensielle skadefølger og betydning for kritisk infrastruktur og kritiske samfunnsfunksjoner er viktige momenter i denne vurderingen.

Innenfor kriteriene for skjermingsverdighet kan det også dreie seg om deler av et objekt som er skjermingsverdig uten at hele objektet faller inn under kriteriene for skjermingsverdig. Deler av et skjermingsverdig objekt kan også ha ulik klassifiseringsgrad.

Ot.prp. nr. 21 (2007-2008) gir viktige føringer for hvordan skjønnet ved utvelgelse av objektene skal utøves. Det blir understreket at det må dreie seg om objekter som etter en skadevurdering må anses helt essensielle for samfunnsviktige interesser. Det må være en forutsetning at ødeleggelse av objektet som sådan kan true vitale nasjonale sikkerhetsinteresser. Objekter som kun har en lokal betydning vil vanskelig kunne sies å falle inn under definisjonen av skjermingsverdig objekt.

Utvelgelse av objekter skal ikke skje i større utstrekning enn nødvendig. I dette ligger at objekter som skal omfattes av bestemmelsene må ha betydning for rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser.

Om forståelsen av begrepet ”skjermingsverdig objekt” vises også til merknader i Ot.prp. nr. 49 (1996-1997) som presiserer hva som kan ligge i definisjonen av skjermingsverdig objekt:

> *”Det forutsettes at aktiviteter i seg selv kan være skjermingsverdige, og vil indirekte kunne dekkes av definisjonen her, ved at stedet hvor aktiviteten foregår pga. aktiviteten vil være et skjermingsverdig objekt.”*
>
> *”Definisjonen vil også i gitte situasjoner dekke bygninger eller områder hvor personer befinner seg, utelukkende som følge av personenes tilstedeværelse, dersom personene for eksempel har en slik funksjon i den nasjonale beslutningsprosessen eller lignende at det vil kunne skade rikets sikkerhet m.v. om deres tiltenkte funksjon elimineres eller på annen måte umuliggjøres eller hemmes som følge av sikkerhetstruende virksomhet.”*

For å kunne utøve en kritisk funksjon ved et objekt, er man ofte avhengig av andre virksomheter. Det er derfor essensielt at man avdekker avhengigheter mellom skjermingsverdige objekt, og hvor sterk avhengigheten er.

Det er en særlig meddelelsesplikt for objekteier overfor andre objekt man er avhengig av. Dette er begrunnet i behovet for å motvirke sårbarheter som følge av den sterke avhengigheten på tvers av virksomheter og ulike sektorer i samfunnet. For at NSM skal ivareta sin koordinerende rolle, er det viktig at meddelelser sendes med gjenpart til NSM.

Det forutsettes at departementene tar hensyn til avhengigheter innen sine forvaltningsområder. NSM og fagdepartementene har et felles ansvar for å koordinere slik at det blir tatt hensyn til avhengighet på tvers av sektorer (tverrsektorielle) ved utvelgelse og klassifisering av objekter.

Loven pålegger departementene å føre register og melde alle skjermingsverdige objekt med angivelse av klassifiseringsdrag til NSM. Som følge av dette, vil NSM utarbeide en oversikt over de innmeldte skjermingsverdige objekter. Denne oversikten sammen med en løpende analyse av tverrsektorielle avhengigheter vil være utgangspunkt for denne type koordinering.

Mangel på substitutter og en sterk samfunnsmessig avhengighet, samt at objektets funksjonssvikt vil påvirke andre samfunnsfunksjoner forsterker behovet for å beskytte objektet.

Vurderinger, analyser og oversikter m.m. som er tilknyttet utvelgelsesprosessen skal graderes etter sitt innhold.

4.4 Ledetråder til vurdering

Hva kan jeg klare meg uten, og hvor lenge? Hva kan jeg *ikke* unnvære?

Sikkerhetsloven § 17 — *Utvelgelse av skjermingsverdige objekter*

Alle virksomheter har en funksjon og en hensikt. Spørsmålet er om virksomheten har funksjoner som gjør at enten hele eller deler av virksomheten kan kategoriseres som skjermingsverdig objekt. Det må først utarbeides en verdivurdering som vil gi svar på spørsmålet. På denne måten vil virksomheten kunne systematisk kunne identifisere hvilke kritiske innsatsfaktorer som understøtter virksomheten. Videre må verdiene klassifiseres etter en skadevurdering ut fra kriteriene i sikkerhetslovens § 17.

Ved å vurdere hvilken verdi et objekt eller en funksjon har for en virksomhet, vil man samtidig få svar på hvor stor risiko virksomhetene er villig til å ta i forhold til beskyttelse av sårbarheter mot potensielle trusler. Tilsvarende kan man også vurdere hvilken verdi objektet vil ha for en potensiell motstander, dette vil si noe om hvor langt vedkommende er villig til å gå for å ramme verdien.

Objektsikkerhetsforskriften søker å avdekke tverrsektorielle avhengigheter og funksjoner av avgjørende betydning for rikets sikkerhet og vitale nasjonale sikkerhetsinteresser. Definisjonen av et skjermingsverdig objekt leder opp til det sentrale i funksjonaliteten. Et mulig utgangspunkt kan være å se objektet i en større sammenheng:

1. Funksjon

Vurder i hvilken grad en sikkerhetstruende virksomhet mot et objekt kan påvirke egen sektor og utover denne. Gjennomfør en dokumenterbar vurderingsprosess før en eventuell beslutning nås. Se redundans opp mot funksjonalitet i normaltilstand. Følgende problemstillinger *kan* vurderes:

- Hva slags utstyr og teknologi trenger virksomheten for å kunne fungere?
- Hvor lang tid kan det ta før virksomheten fungerer igjen etter et avbrudd?
- Hvilke kortsiktige og langsiktige konsekvenser får et avbrudd?
- Hvilke alternative ressurser finnes?
- Hvilke tredjeparter blir skadelidende om virksomheten rammes?
- Hvilken kunnskap omkring de oppgaver som utføres er unik i virksomheten?
- Hvordan er data og annen driftsnødvendig informasjon tilgjengelig? Hvordan dubleres dette?
- På hvilken måte kan virksomhetens nettverk kommunisere med andre nettverk, eller er avhengig av en spesiell datateknisk drift?

2. Sikkerhetstruende hendelser

Uavhengig om virksomheten har skjermingsverdige objekt eller ikke, er innføring av hendelsesrapportering på mulig sikkerhetstruende hendelser et godt verktøy for å avdekke sårbarheter. Fravær av hendelsesrapportering kan tyde på en lav sikkerhetsbevissthet, da selve innrapporteringen bidrar til en generell økning i sikkerhetsbevisstheten. Hendelsesrapportering er et effektivt verktøy for å kunne avdekke sikkerhetstilstanden i en

virksomhet, og kan gi gode indikasjoner på *hvor* sikkerhetstiltak vil kunne ha størst effekt. God kultur for rapportering av uønskede hendelser bør oppmuntres i virksomheten.

Tidligere hendelser i egen og sammenlignbar virksomhet kan også bidra til å avdekke mulige sårbarheter mot sikkerhetstruende hendelser. Følgende problemstillinger *kan* vurderes:

- På hvilken måte kan virksomhetens informasjon misbrukes innen terrorisme, sabotasje og spionasje?
- Hvilken mulighet har, og hvordan kan medarbeidere rapportere om mulig sikkerhetstruende hendelser?
- Hvem ved virksomheten har tilgang til essensiell infrastruktur, og hvordan reguleres denne tilgangen?
- Hvilken informasjon på åpne nett om virksomheten er tilgjengelig?
- Hva er virksomhetens sårbarhet ved en eventuell endret lokalisering?
- På hvilken måte er virksomheten forbundet med et omstridt arbeidsfelt eller profilerte personer?
- Er det tidligere kommet trusler mot virksomheten eller dets personell? Hva med tilsvarende virksomheter og trusler?
- Hvordan beskrives det mulig skjermingsverdige objektets plassering – ligger det i nærhet av viktig infrastruktur (knutepunkter) eller andre mulige terror/sabotasjemål?

3. Sikringstiltak

Nesten alle virksomheter har noen sikringstiltak i funksjon. Ikke alle virksomheter vil ha et behov for synlige sikringstiltak. NSM understreker viktigheten av at virksomheter er bevisst på hvilken restrisiko som er akseptert. Se også kapittel 8 for en mulig prosessgjennomgang av grunnsikring. Følgende problemstillinger *kan* vurderes opp mot ønskede sikringstiltak:

- Hvordan er nøkkelpersonell sikret ved virksomheten?
- Hvilken områdesikkerhet er iverksatt for en eventuell sårbar bygningsmasse?
- Hvilke nye metoder eller teknologi kan forbedre eksisterende sikkerhetstiltak?
- Hvordan er eksisterende sikkerhetstiltak dimensjonert for planlagte utvidelser?
- Er virksomheten tilgjengelig ved eller gjennom allmenn/offentlig ferdsel?
- Er krav til underleverandørers sikkerhetsstandarder blitt beskrevet? På hvilken måte er disse i samsvar med virksomhetens egne sikkerhetsstandarder?
- Hvilke synlige sikringstiltak eksisterer?
- I hvilke situasjoner er virksomheten mer utsatt enn andre?

5 Klassifisering av skjermingsverdig objekter

5.1 Utgangspunkt

Departementene skal klassifisere de skjermingsverdige objektene innen sine myndighetsområder.

Sikkerhetsloven § 17a – *Klassifisering av skjermingsverdig objekt*
Forskrift om objektsikkerhet § 2-2 *- Klassifiseringen*

Klassifisering skal angi den sikkerhetsmessige verdien objektet har i forhold til hvor alvorlige skadefølger det vil få dersom objektet får redusert funksjonalitet, blir utsatt for skadeverk eller rettstridig overtatt. Beskyttelsestiltakene knyttet til objektet blir større jo høyere objektet er klassifisert.

Klassifiseringssystemet skal anvendes på de objekter som allerede er utpekt som skjermingsverdig objekt. Klassifisering er et verktøy for å bestemme verdi på de objekter som er definert som skjermingsverdige objekter.

5.2 Fastsettelse av klassifiseringsgrad

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

Sikkerhetsloven § 17a – *Klassifisering av skjermingsverdig objekt*
Forskrift om objektsikkerhet § 2-2 *- Klassifiseringen*

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

Utvelgelse og klassifisering er to ulike vurderinger, selv om de i stor grad vil bygge på det samme vurderingsgrunnlaget. Utvelgelse består i å finne ut hva som er et skjermingsverdig objekt. Klassifiseringsprosessen til objektet består i at departementet fastsetter hvor alvorlige skadefølger redusert funksjonalitet, skadeverk, ødeleggelse eller rettsstridig overtakelse vil få for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.

Det skal benyttes tre klassifiseringsnivåer for skjermingsverdige objekter:

- **MEGET KRITISK** nyttes dersom det kan **få helt avgjørende skadefølger** for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende

- **KRITISK** nyttes dersom det **alvorlig kan skade** rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende

- **VIKTIG** nyttes dersom det **kan skade** rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende

Det er bare de deler av et objekt som er skjermingsverdig som skal klassifiseres. Innenfor et avgrenset område kan det være skjermingsverdige objekt med forskjellig klassifisering.

Ikke alle skjermingsverdige objekter vil kreve like strenge beskyttelsestiltak. Det er derfor vesentlig å finne riktig klassifiseringsnivå.

Sikkerhetsloven har et krav til forholdsmessighet i de tiltak som iverksettes. For høy klassifisering vil medføre overdreven ressursbruk som kunne vært anvendt på en mer hensiktsmessig måte. Videre skal sikringstiltakene være minst mulig inngripende overfor objekteier, ansatte og brukere av objektet Det skal derfor ikke brukes høyere klassifiseringsgrad enn nødvendig. På den andre side skal ikke kostnader være et argument for å gi et objekt en lav klassifisering.

I vurderingen skal det også tas hensyn til gjensidige avhengigheter og objektets totale betydning dersom det har flere samfunnsmessige funksjoner.

5.3 Registrering og koordinering

Sikkerhetsloven § 17 a (2) – *Klassifisering av skjermingsverdig objekt*
Forskrift om objektsikkerhet § 2-4 *– Registrering og koordinering*

De enkelte departementer skal føre register over skjermingsverdige objekter og klassifiseringen av disse innen eget myndighetsområde. Departementet skal kunne fremskaffe opplysninger i samsvar med de rapporteringskriteriene som NSM angir (se vedlegg A.1). Departementets oversikt over skjermingsverdige objekter vil være et grunnlag for NSMs tilsyn på utvelgelse og klassifisering skjer etter lovens intensjon. For øvrig avgjør departementet selv hvilken informasjon et slikt register skal inneholde. Registeret skal sikkerhetsgraderes etter innhold, ref. objektsikkerhetsforskriften § 2-4. NSM vil i denne sammenheng vise til bestemmelser for informasjonssikkerhet og NSMs veileder i verdivurdering[8].

Alle skjermingsverdige objekter skal meldes til NSM med angivelse av klassifiseringsgrad.

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

At et objekt er sikkerhetsklassifisert er ugradert informasjon. Informasjon **om** skjermingsverdige objekter vil derimot normalt være skjermingsverdig. Eksempelvis kan det være behov for å skjerme informasjon om betydning, kapasitet, sårbarhet og sikkerhetstiltak med mer. Merk at opplysning om hvilken klassifiseringsgrad et skjermingsverdig objekt har, skal sikkerhetsgraderes minst BEGRENSET. En oversikt over samtlige eller større antall av skjermingsverdige objekter med angivelse av klassifisering, skal sikkerhetsgraderes minst KONFIDENSIELT.

[8] Veiledning i verdivurdering:
https://www.nsm.stat.no/Documents/Veiledninger/Veiledning%20i%20verdivurdering%20200903.pdf

NSM vil årlig be om innrapportering fra departementene. Objekteiere skal ikke rapportere direkte til NSM, med mindre objekteier er et departement. NSM fastsetter nærmere prosedyrer og format for innrapportering.

6 Beskyttelse av skjermingsverdige objekter

6.1 Utgangspunkt

Objekteier plikter å beskytte objektet med sikkerhetstiltak.

Sikkerhetsloven § 3 *— Definisjoner*
Sikkerhetsloven § 17 b *— Plikt til å beskytte skjermingsverdige objekt*
Forskrift om objektsikkerhet § 3-1 *– Generelle krav til beskyttelsen*
Forskrift om objektsikkerhet § 4-2 *– Internkontroll*
Forskrift om sikkerhetsadministrasjon § 3-4 *– Instrukser for rutiner og prosedyrer*

Objekteier plikter å beskytte objektet med sikkerhetstiltak som skal utgjøre en grunnsikring av det skjermingsverdige objektet til enhver tid. Sikkerhetstiltakene vil være defensive egenbeskyttelsestiltak. Grunnsikringen skal være en kombinasjon av barrierer, deteksjons-, verifikasjons- og reaksjonstiltak. I tillegg stilles det spesifikt krav om:

- tiltak mot etterretningsvirksomhet,
- tilrettelegging for beskyttelse av IKT-infrastruktur,
- tiltak mot elektromagnetisk puls og høyfrekvente mikrobølger,
- tilrettelegging for bruk av sikringsstyrker,
- rutiner knyttet til sikkerhetsklarering, autorisasjon,
- rutiner i forbindelse med besøk

Sikkerhetstiltakene skal planlegges, gjennomføres og vedlikeholdes som permanent grunnsikring for objektene.

Objekteiers grunnsikring må sees i sammenheng med eventuelle tiltak fra politiet (med hjemmel i politilovens § 2) og Forsvaret (med hjemmel i nøkkelpunktdirektivet) i forhold til beskyttelse av objektet med sikringsstyrker.

Objekteier skal utføre internkontroll etter forskrift om sikkerhetsadministrasjon. Dette innebærer at objekteier skal foreta risikovurdering og intern sikkerhetsrevisjon, som igjen danner grunnlag for sikkerhetstiltak. Faktorene *verdi* (det man vil beskytte ved objektet), *sikkerhetstrussel* og *sårbarhet* utgjør til sammen risikobildet. Kjennskap til risikobildet er en forutsetning for å kunne etablere defensive, forebyggende sikkerhetstiltak på en hensiktsmessig måte.

En del av sikringstiltakene må iverksettes som grunnsikring i en normalsituasjon uten at noen konkret trussel foreligger. Det vil typisk være tiltak som skal forebygge mot angrepstyper som det ikke kan forventes en varslingstid for, for eksempel adgangskontroll og foliering av vinduer.

Enkelte tiltak kan man imidlertid vente med å iverksette. Dette kan også være hensiktsmessig av effektivitets-, økonomiske og rettssikkerhetsmessige hensyn. Slike tiltak kan reserveres som påbygningstiltak i et beredskapssystem, for ved behov å kunne øke

sikringsnivået. Eksempler på slike beredskapstiltak kan blant annet være tilordning av sikringsstyrker. Virksomheten må beskrive disse tiltakene i sine sikringsplaner.

Objekteier skal også planlegge for å gjennomføre påbygging av grunnsikringen ved økt risiko. Det er utarbeidet egne dokumenter som gir nærmere veiledning og tiltak på dette området[9].

Forskrift om sikkerhetsadministrasjon krever at virksomhetene skal ha oversikt over gjeldende sikkerhetstiltak og påbyggende tiltak som kan iverksettes ved økt risiko. Forholdet mellom virksomhetens beredskapsorganisasjon og sikkerhetsorganisasjonen skal være avklart. Dette skal dokumenteres i en beredskapsplan, som skal øves minst en gang i året.

6.2 Objektsikkerhet og sikkerhetstruende virksomhet

Sikkerhetsloven § 3 nr.3 – *Definisjoner*
Sikkerhetsloven § 3 nr.4 – *Definisjoner*
Sikkerhetsloven § 3 nr.5 – *Definisjoner*
Sikkerhetsloven § 21 *– Vurderingsgrunnlaget for sikkerhetsklarering*
Forskrift om objektsikkerhet § 3-2 *– Tiltak mot etterretningsaktivitet*

I objektsikkerhetsarbeidet skal man ta utgangspunkt i at sikkerhetstruende virksomhet kan utnytte mangler ved sikkerheten og hvilke konsekvenser det vil få hvis objektet utsettes for spionasje, sabotasje og terrorisme. Ved etablering av forebyggende sikkerhetstiltak bør man ta utgangspunkt i mulige trusselaktører med en betydelig kapasitet. Nærmere informasjon om trusselaktører og trusselnivået finnes i trusselvurderingene til Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten. Trusselaktørene må som regel skaffe seg informasjon om det de ønsker å angripe for å forberede sabotasje eller terrorhandlinger. Informasjon om objektet må derfor beskyttes.

a) Sabotasje er tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering. Sabotasje kan eksempelvis brukes til å understøtte både spionasje og terrorisme, gjennom enten å avdekke svakheter, responstid og responshandling eller å forsterke effekten av andre angrep.

b) Spionasje er ulovlig innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt. Spionasje utgjør en trussel mot nasjonale interesser. Spionasjeaktiviteten har ikke sunket etter den kalde krigen, og tekniske nyvinninger har gjort spionteknologi kommersielt tilgjengelig. Der militære og politiske mål har vært fokus for spionasje, har også andre felt som forskning, industri, luftfart og energi også i økende grad vært spionasjemål.

Spionasje kan foregå både fra utsiden og innsiden i en virksomhet. Også egne ansatte kan spionere mot egen virksomhet. Det kan ha særlig stor verdi for aktørene bak dersom virksomheten har skjermingsverdig informasjon. Noen kan bli rekruttert og andre blir manipulert til å oppgi informasjon. Rekrutterte spioner i egen virksomhet finner gjerne sin motivasjon innen enten økonomiske interesser, ideologisk overbevisning, egosentrisme eller gjennom å bli utsatt for press. Annen

[9] Sikkerhets- og beredskapstiltak mot terrorhandlinger, utgitt av NSM, PST og POD i 2010 (sehttps://www.nsm.stat.no/Documents/Temahefter/Sikkerhets-%20og%20beredskapstiltak%20mot%20terrorhandlinger.pdf), kapittel VI i Beredskapssystem for Forsvarssektoren (BFF) [gradert BEGRENSET], og kapittel VI i Sivilt Beredskapssystem (SBS) [gradert BEGRENSET].

informasjon kan også innhentes gjennom sosial manipulering, hvor en gjennom hjelpsomhet og serviceinnstilling uforvarende oppgir informasjon om virksomhetens rutiner og personell.

c) Terrorhandlinger er ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål. Terrorismens mål eller virkemiddel er å spre frykt og usikkerhet, og en terroraksjon vil derfor søke å være uventet og kan ramme hvilken som helst virksomhet.

6.3 Krav til grunnsikring

Grunnsikringen skal være tilpasset det enkelte objekt.

Sikkerhetsloven § 17 a — *Klassifisering av skjermingsverdige objekter*
Sikkerhetsloven § 17 b — *Plikt til å beskytte skjermingsverdige objekt*

De skjermingsverdige objektenes art, omfang og verdi vil være svært ulike. Derfor har det ikke vært hensiktsmessig å foreslå krav om konkrete sikkerhetstiltak som kan anvendes på enhver type objekt. Sikkerhetstiltakene må tilpasses det enkelte objekts særegenheter. Det er derfor lovfestet kun funksjonelle krav til sikringen.

Grunnsikringen skal oppfylle kravene innen den aktuelle klassifiseringsgrad for objektet. Objekteier plikter å beskytte skjermingsverdige objekter med en kombinasjon av sikkerhetstiltak som i sum tilfredsstiller følgende krav:

- Objekt klassifisert MEGET KRITISK skal beskyttes slik at tap av funksjon, ødeleggelse og rettsstridig overtakelse **avverges**.

- Objekt klassifisert KRITISK skal beskyttes slik at tap av funksjon og ødeleggelse **begrenses**, og rettsstridig overtakelse av vesentlige funksjoner **avverges**.

- Objekt klassifisert VIKTIG skal beskyttes slik at tap av vesentlig funksjon og ødeleggelse **begrenses**.

Tiltakene skal bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon som er tilpasset det enkelte objekt.

– *Barrierer* skal forhindre eller redusere muligheten for at sikkerhetstruende hendelser kan inntreffe. Barrierene kan være av fysisk (for eksempel vegger, murer, gjerder, dører med videre), elektronisk (kryptologi og brannmurer, adgangskontroll, overvåkningssensorer og lignende) eller administrativ art (sikkerhetsklarering og autorisasjon, adgangsrutiner, sikringsplaner og – prosedyrer).

– *Deteksjonstiltak* skal etableres for å avdekke hvorvidt etablerte barrierer brytes eller blir forsøkt brutt fra innsiden eller utsiden. Eksempel her kan være overvåking av sensorer og alarmsystemer.

– *Verifikasjonstiltak* skal ta sikte på å etablere en situasjonsforståelse hvis en sikkerhetstruende hendelse inntreffer. Tiltakene skal ha som formål å kunne identifisere og avdekke aktører, identifisere skadeomfang og identifisere de midler som eventuelt er anvendt av en aktør. Eksempel på dette kan være prosedyrer for vaktmannskaper eller handlingsrutiner om mistanke ved innbrudd i et IKT-system.

– *Reaksjonstiltak* skal sikre opprettholdelse av objektets funksjonalitet ved en sikkerhetstruende hendelse, eller sikre forutsetninger for gjenopprettelse av funksjonalitet etter en slik hendelse. Eksempler på dette kan være bistand fra andre etater, relokalisering eller innkalling av ekstra personell ved overgang til nødrutiner. Aktuelle reaksjonstiltak skal være forberedt som en del av grunnsikringen.

For ulike typer skjermingsverdige objekter vil det kreves ulik vektlegging og kombinasjoner av disse sikkerhetstiltakene tilpasset det enkelte objekt (barriere, deteksjon, verifikasjon og reaksjon). Objektsikkerhetsforskriften forutsetter at utvikling av tiltak ved ulike objekttyper og normer for tiltak må skje innen den enkelte sektor. NSM har utarbeidet en veileder i fysisk sikring som vil kunne være til hjelp i dette arbeidet[10]. Sikringshåndboka, utgitt av Forsvarsbygg, vil også kunne være et nyttig hjelpemiddel for å etablere sikringstiltak.

Hvordan sikringstiltakene utformes er i stor grad avhengig av hvordan objektet er konstruert. Tiltakenes utforming vil imidlertid også i stor grad være avhengig av hvordan man tenker seg at eventuelle angrep eller sikkerhetsbrudd vil kunne skje. Det er overlatt stor grad av skjønn til objekteierne, men NSM forutsetter at objekteiers vurderinger dokumenteres i en risikovurdering.

For eksempel vil det være slik at georedundans, i form av geografisk spredning av infrastruktur som understøtter en funksjon, bidrar til å redusere verdien av det enkelte objekt, og dermed risikoen til funksjonen objektet understøtter. Dette er derfor et tiltak som gjør at objekteier kan oppnå et akseptabelt risikonivå, med mindre inngripende fysiske sikringstiltak på det enkelte objekt.

Selv om objekteier skal ta utgangspunkt i at mulige trusselaktører er fremmede makter eller internasjonale terrororganisasjoner, betyr ikke dette at grunnsikringstiltakene på det enkelte objekt klassifisert som VIKTIG eller KRITISK må dimensjoneres for å hindre fullstendig ødeleggelse av spesialstyrker. Det funksjonelle kravet til grunnsikringstiltak for VIKTIGE og KRITISKE objekter er kun at tap av funksjon og ødeleggelse *begrenses*, jf. sikkerhetsloven § 17b. I tillegg er det slik at fremmede staters spesialstyrker, som har høyere kapasitet enn terrororganisasjoner, er et aktuelt virkemiddel (trussel) først ved et relativt høyt konfliktnivå av utenrikspolitisk art. Et slikt konfliktnivå vil typisk utvikle seg over noe tid, slik at det vil være mulig å planlegge med at sikringsstyrker vil kunne utplasseres i tide ved de objektene der dette er et prioritert og egnet tiltak. Med terrorhandlinger vil det kunne være annerledes. Terrorhandlinger kan skje uten forvarsel eller med så kort varslingstid at grunnsikringen i større grad må ta høyde for trusselen.

Der grunnsikringstiltak kommer i konflikt med pålagte informasjonssikkerhetstiltak etter sikkerhetslovens kapittel 4, skal det etableres tilpassede sikkerhetstiltak. Et eksempel kan være et objekt klassifisert som KRITISK eller MEGET KRITISK med vaktmannskap som ivaretar adgangskontroll. Vaktmannskapet som her foretar områdesikring uten tilgang til objektet, vil ikke nødvendigvis være klarert og autorisert. Ved at vaktmannskapet her er kjent med virksomheten, vil disse kunne få kunnskap om sårbarheter ved objektet. Tilsvarende sårbarhetsinformasjon i form av et dokument ville vært gradert og medført behov for sikkerhetsklarering og autorisasjon for å få tilgang til dokumentet. Et kompenserende sikkerhetstiltak vil kunne være å inngå avtale om faste vaktmannskap som skal være klarert og autorisert for den skjermingsverdige informasjonen, selv om de ikke har tilgang. Tilpassede sikkerhetstiltak som avviker fra sikkerhetslovens fjerde kapittel, skal forelegges NSM for godkjenning før de gjennomføres.

[10] Veiledning i fysisk sikring mot ulovlig inntrengning:
https://www.nsm.stat.no/Documents/Veiledninger/Veiledning%20i%20Fysisk%20sikring%20mot%20ulovlig%20inntrengning%20v2.pdf

Virksomheten må som en del av grunnsikringstiltakene ha rutiner for mottak av sikringsstyrker og beredskapspersonell, som hindrer at slik virksomhet kommer i konflikt med adgangsbegrensninger til skjermet objekt eller informasjon.

For en konkretisert gjennomgang av iverksetting av grunnsikringstiltak, se kapittel 8.

6.4 Tiltak mot etterretningsvirksomhet

Objekteier skal beskytte objektet mot informasjonsinnhenting som kan ha til hensikt å forberede sabotasje eller terrorhandling.

Forskrift om objektsikkerhet § 3-2 *– Tiltak mot etterretningsaktivitet*

Tilgang til informasjon om samfunnets sårbare punkter styrker evnen hos ondsinnede aktører til å utføre sikkerhetstruende virksomhet. Informasjon om sårbarheter kan i visse tilfelle bli en utløsende faktor for et anslag mot et objekt.

Sikkerhetstiltakene skal ta sikte på i nødvendig grad å redusere muligheten for uønsket innhenting av opplysninger om funksjoner, betydning, kapasitet, sårbarhet og sikkerhetstiltak knyttet til objektet.

Eksempler på aktuelle tiltak mot etterretningsvirksomhet kan være sikkerhetsgradering av informasjon om objektets funksjon og sikringstiltak, bruk av godkjente og oppdaterte informasjonssystemer, autorisasjonssamtaler, kamuflering av infrastruktur, tiltak mot avlytting og avlesing, tiltak mot opptak fra luftbårne og satellittbaserte sensorsystemer, bevissthet omkring sikkerhetskultur i virksomheten, vakthold, adgangskontroll med mer. NSM viser til forskrift om informasjonssikkerhet kapittel 9 og 10 om sikring mot avlytting. NSM har utarbeidet relevante veiledere for denne forskriften[11]. Se også punkt 6.9. om rutiner for håndtering av besøk.

Det forutsettes at en del kjerneinformasjon om skjermingsverdige objekter vil falle inn under graderingsbestemmelsene i sikkerhetsloven kapittel 4 og informasjonssikkerhetsforskriften. Dette kan for eksempel gjelde risikovurderinger, plantegninger, tekniske spesifikasjoner, beskrivelser av sikkerhetstiltak, beskrivelser av konstruksjon og virkemåte, samt beredskapsplaner for beskyttelse og bruk av objektet i kriser. At informasjon om objektet er skjermingsverdig etter sikkerhetsloven, medfører at informasjonen må beskyttes med hensyn til hvordan den håndteres, oppbevares og lagres. Videre forutsetter tilgang til slik informasjon at personer er sikkerhetsklarert og autorisert.

Sikkerhetsklarering og autorisasjon gir objekteiere en mulighet til å bedre den daglige sikkerhetsmessige ledelse. Dette ivaretas da gjennom en gjensidig forpliktelse til å opplyse om forhold som kan ha sikkerhetsmessig betydning for virksomheten knyttet til objektet.

Når informasjon om et skjermingsverdig objekt må beskyttes av sikkerhetsmessige grunner, skal den sikkerhetsgraderes etter sitt innhold.

6.5 Tilrettelegging for beskyttelse av IKT-infrastruktur

Forskrift om objektsikkerhet § 3-3 *– Tilrettelegging for beskyttelse av IKT-infrastruktur*

Mange skjermingsverdige objekter er avhengige av datanettverk og internettinfrastruktur for å fungere. Deler av den IKT-baserte infrastrukturen kan i seg selv også betraktes som

[11] Se NSMs oversikt over veiledninger: https://www.nsm.stat.no/Publikasjoner/Veiledninger2/

skjermingsverdig objekt. Eksempelvis kan et angrep som rettes mot kritiske punkter i den norske internettinfrastrukturen kunne ramme tverrsektorielt og få store følger for virksomheter som er avhengige av kommunikasjonssystemer som går over internett.

For å kunne avdekke forberedelser til og gjennomføring av angrep, er det nødvendig å analysere internettrafikken på bred basis. For å kunne gjøre dette, er det etablert et nasjonalt nettverk av sensorer for deteksjon av angrep via internett. Systemet kalles varslingssystem for digital infrastruktur (VDI). Det er NSM som drifter VDI og analyserer informasjonen fra sensorene. Sensorene er plassert hos forskjellige virksomheter med samfunnskritiske funksjoner, og gjør at det kan leveres et bilde i sann tid av trafikken på internett. Et korrekt situasjonsbilde er bare mulig gjennom at informasjon fra virksomheter i ulike sektorer hentes inn. I situasjoner med økt risiko kan det være avgjørende å styrke muligheten for å tilpasse og styrke innhentingskapasiteten. Bestemmelsen tar sikte på å etablere et grunnlag for å sikre nødvendig representativitet i dette situasjonsbildet. Det understrekes at VDI er et tillegg til egen digital grunnsikring.

Dersom tilknytning til internett utgjør en sårbarhet for sikkerheten til et skjermingsverdig objekt, kan fagdepartementet i samråd med objekteier bestemme at det skal søkes NSM om tilknytning til VDI.

NSM har nærmere retningslinjer for hvordan tilknytning til VDI settes opp og forvaltes.

For ytterligere informasjon om tilknytning til VDI, kontakt postmottak@nsm.stat.no, www.nsm.stat.no og tlf (+47) 67 86 40 00.

6.6 Tiltak mot elektromagnetisk puls og høyfrekvente mikrobølger

Forskrift om objektsikkerhet § 3-4 *– Tiltak mot elektromagnetisk puls og høyfrekvente mikrobølger*
Forskrift om sikkerhetsadministrasjon kap 4

Elektromagnetisk puls og høyfrekventerte mikrobølger (EMP/HPM) er trusler som det fokuseres på i forbindelse med sabotasje og terrorhandlinger. Kunnskap og våpen for bruk av EMP/HPM er tilgjengelige og kan brukes til å slå ut IKT-utstyr permanent eller for en periode. Teknologi- og samfunnsutviklingen har medført en særlig sårbarhet i forhold til denne trusselen.

Den enkelte sektor vil være nærmest til å vurdere hva som kan aksepteres av risiko når det gjelder trusselen fra EMP/HPM. Det kan være en utfordring å finne eksakte krav til EMP/HPM-sikring som skal ha effekt for alle typer objekter i alle sektorer. Ved gjennomføring av risikovurdering og sikkerhetsrevisjon skal derfor behovet for å beskytte elektroniske systemer mot elektromagnetisk puls (EMP) og høyfrekvente mikrobølger (HPM) vurderes. Objekteier pålegges en plikt til å vurdere risikoen objektet er utsatt for, herunder trusselnivå og sårbarhet vedrørende EMP/HPM, og ut i fra dette iverksette nødvendige tiltak.

Forsvarsbygg og Forsvarets forskningsinstitutt har kompetanse på hvordan bygningsmasse og elektronisk infrastruktur kan beskyttes mot elektromagnetisk puls og høyfrekvente mikrobølger.

6.7 Tilrettelegging for bruk av sikringsstyrker

Forskrift om objektsikkerhet § 3-5 *– Tilrettelegging for bruk av sikringsstyrker*

Objekteier plikter å legge til rette for at sikringsstyrker kan forberede, øve og gjennomføre tiltak på og ved objektet for beskyttelse der dette blir vurdert som nødvendig.

Denne plikten må sees i sammenheng med Forsvarets utvelgelse av nøkkelpunkter (i henhold til nøkkelpunktdirektivet) og politiets utvelgelse av særskilte objekter etter politilovens § 2.

6.8 Sikkerhetsklarering og autorisasjon

Forskrift om objektsikkerhet § 3-6 *– Sikkerhetsklarering og autorisasjon*

Vedkommende departement kan bestemme at enhver som skal gis permanent adgang til skjermingsverdig objekt klassifisert som KRITISK eller MEGET KRITISK skal være autorisert og sikkerhetsklarert før slik adgang gis.

Dersom departementet stiller krav om klarering, skal det kreves klarering for KONFIDENSIELT eller høyere for objekt klassifisert som KRITISK. Objekt klassifisert MEGET KRITISK krever klarering HEMMELIG eller høyere.

Dersom objekteier mener det bør stilles krav til sikkerhetsklarering for person som skal ha permanent adgang til objektet, må dette nærmere begrunnes. Sikkerhetsklarering skal ikke foretas der dette ikke anses som et egnet virkemiddel. Andre sikringstiltak skal iverksettes først, dersom de kan kompensere bruk av sikkerhetsklarering. Dette av hensyn til å begrense antall klarerte personer til et nødvendig minimum.

Det følger av forarbeidene til forskriften at hovedregelen bør være at den som skal gis permanent tilgang til objekter klassifisert KRITISK eller MEGET KRITISK er sikkerhetsklarert[12]. NSM anbefaler at personell som skal ha permanent adgang til skjermingsverdige objekter klassifisert som VIKTIG, som hovedregel bør være autorisert for BEGRENSET. En slik autorisasjon kan gjøres uten å gjennomføre en sikkerhetsklarering. Personellet skal da ha autorisasjonssamtale hvor man skal bli forklart sikkerhetsregelverket knyttet til objektet. Samtalen er blant annet en anledning til å skape en fremtidig gjensidig dialog mellom den autoriserte og virksomheten om den daglige sikkerheten ved objektet. Det vises her til autorisasjonshåndboka som er tilgjengelig på NSMs nettsider[13].

NSM skal informeres om hvilke skjermingsverdige objekter det kreves sikkerhetsklarering for. Dette kan meldes inn innen rammen av utvelgelse og identifisering av skjermingsverdige objekter.

I enkelte tilfeller vil sikkerhetsklarering være et uforholdsmessig krav eller ikke være et egnet virkemiddel, selv for høyt klassifiserte objekter. Departementene er derfor gitt fullmakt til å foreta denne avveiningen. Utfordringen blir å sikre en ensartet praksis innenfor den enkelte samfunnssektor, men med rom for at særegne behov kan bli tatt hensyn til på grunnlag av en saklig begrunnelse. NSM vil kunne bistå departementene på dette området. Andre kompenserende sikkerhetstiltak, som for eksempel soneinndeling med adgangskontroll, må først vurderes iverksatt for å redusere behovet for klareringer.

I de tilfeller der personer uten sikkerhetsklarering har permanent tilgang til skjermingsverdig objektet, må det utarbeides hensiktsmessige rutiner for å skjerme sikkerhetsgradert informasjon (beredskapsplaner, risikovurderinger og lignende). Det samme gjelder for besøkende.

NSM gjør oppmerksom på at personell i nødetater ikke nødvendigvis er sikkerhetsklarerte. Det må skilles mellom øvelse og reell nødssituasjon. I forbindelse med øvelser, vil adgang til

[12] Ot.prop. nr 21 (2007-2008), side 38.

[13] Håndbok i autorisasjon og autorisasjonssamtale: https://www.nsm.stat.no/Publikasjoner/Handboker/

objektet for sikringstyrker og personell i nødetater kunne forberedes gjennom ulike kompenserende sikringstiltak.

I en reell nødssituasjon vil reglene om nødautorisasjon gjelde så langt situasjonen tillater det. Det vises til reglene om nødautorisasjon i forskrift om personellsikkerhet § 5-3. Liv og helse i en nødssituasjon går foran sikkerhetsmessige hensyn i medhold av sikkerhetsloven.

Beskyttelse av skjermingsverdig informasjon og materiale som virksomheten har et særskilt behov for å berge i en nødssituasjon, må foregå i samarbeid med og under ledelse av den relevante nødetaten.

Eventuelle sikkerhetsbrudd som oppstår som følge av nødssituasjoner må håndteres i etterkant, i henhold til gjeldende regler for dette.

6.9 Rutiner for håndtering av besøk

Forskrift om objektsikkerhet § 3-6 *– Sikkerhetsklarering og autorisasjon*

Besøkende ved det skjermingsverdige objektet skal ledsages av en autorisert person for tilgang til objektet. Besøkende som ledsages av autorisert representant behøver ikke sikkerhetsklareres. Begrepet besøkende vil i denne forbindelse også omfatte leverandører, servicepersonell etc. som eventuelt ikke har sikkerhetsklarering.

Før besøkende gis adgang til skjermingsverdig objekt eller del av objekt klassifisert som KRITISK eller MEGET KRITISK, skal det forsikres om at deres identitet er korrekt.

Alle besøkende skal registreres, og registreringen skal oppbevares i minimum fem år. Et eksempel på en registrering er en besøksprotokoll hvor man fører inn dato og tidspunkt(er) for besøk, navn på besøkende og følgeperson med signatur. Det bør tilstrebes duplisering av besøksprotokoll for å sikre oppbevaringen av denne i henhold til objektsikkerhetsforskriften.

For representanter for annen stat, internasjonal organisasjon eller utenlandsk rettssubjekt skal det også forsikres om at disse faktisk representerer vedkommende stat, organisasjon eller utenlandske rettssubjekt. Dette gjøres eksempelvis ved å be om dobbel legitimasjon (pass og gyldig identitetskort) med bilde. Det bør også tilstrebes å innhente autentisering fra vedkommendes arbeidsgiver, ved å kontakte dem i forkant av besøket. Det vises også til de sikkerhetsavtalene Norge har inngått med fremmede stater/internasjonale organisasjoner, med bestemmelser om prosedyrer for gjennomføring av denne type besøk.

Det enkelte departement kan fatte beslutning om nærmere sikkerhetsprosedyrer for godkjenning og gjennomføring av besøk.

7 Administrative bestemmelser

7.1 Kostnadsdekning og dispensasjon fra tiltak

Forskrift om objektsikkerhet § 4-1 – *Iverksettelse av tiltak – kostnader og dispensasjon*

Objekteier skal dekke egne kostnader som følge av tiltak eller pålegg i eller i medhold av sikkerhetslovens kapittel 5 og objektsikkerhetsforskriften.

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

7.2 Internkontroll

Forskrift om objektsikkerhet § 4-2 – *Internkontroll*

Objekteier skal utføre internkontrolltiltak i samsvar med forskrift om sikkerhetsadministrasjon (Forskrift av 29. juni 2001 nr 723).

For mer informasjon vedrørende internkontroll vises det til NSMs veileder i sikkerhetsadministrasjon[14].

7.3 Tilsyn

Forskrift om objektsikkerhet § 4-3 – *Tilsyn og påleggskompetanse*

Tilsynsorganer med ansvar for forebyggende sikkerhet i en sektor skal føre tilsyn med at sikkerhetstiltakene hos objekteierne tilfredsstiller kravene i sikkerhetslovens kapittel 5 og objektsikkerhetsforskriften.

Ansvarsprinsippet ligger til grunn for arbeidet med sikkerhet. Dette innebærer at tilsynsmyndighetene med særlig ansvar innen bestemte sektorer, må føre tilsyn med at bestemmelser som gjelder innenfor egen sektor blir etterlevd. Dette vil i praksis også si at disse tilsynsmyndighetene har ansvaret for å påse at de konkrete tiltakene som etableres, er i overensstemmelse med de krav som stilles. Det må derfor etableres gode samarbeidsrutiner mellom NSM og sektortilsynene om oppfølgingen av objektsikkerhetsarbeidet.

NSM skal føre tilsyn med at utvelgelse og klassifisering av skjermingsverdige objekter skjer i henhold til sikkerhetsloven og objektsikkerhetsforskriften. NSM har i tillegg et tilsynsansvar av en mer overordnet og sektorovergripende karakter. NSM vil ivareta tilsyn med objekter i sektorer der det ikke finnes sektortilsyn med et dekkende regelverk.

7.4 Frister

Forskrift om objektsikkerhet § 5-1 – *Ikrafttredelse*

[14] Veiledning i sikkerhetsadministrasjon:
https://www.nsm.stat.no/Documents/Veiledninger/Veiledning%20i%20sikkerhetsadministrasjon%20v1.0.pdf

Første gangs fastsettelse av sikkerhetsklassifisering og vurdering av tiltak mot etterretningstrussel i forbindelse med klassifisering skal skje senest 2 år etter ikrafttredelsen av regelverket.

Gjennomføringen av sikkerhetstiltak på bakgrunn av fastsatt sikkerhetsklassifisering mv. skal skje så raskt som mulig, og senest 3 år etter ikrafttredelsen.

Opprettelse av internkontrollsystem skal skje senest 3 år etter ikrafttredelsen.

NSM vil oppfordre berørte virksomhet med å starte opp dette arbeidet umiddelbart, da prosessen vil være tidkrevende.

7.5 Klageadgang

Forskrift om objektsikkerhet § 4-4 – *Klage*

Det er kun rettssubjekt underlagt sikkerhetsloven som ikke er forvaltningsorgan, som kan påklage vedtak etter denne forskrift der det enkelte departement er førsteinstans. Klageinstans er Kongen i statsråd.

8 Fastsetting av grunnsikringskrav

Grunnsikringen skal være tilpasset det enkelte objekt. En risikoanalyse skal danne grunnlag for fastsettelse av sikringstiltak.

Sikkerhetsloven § 17 b *– Plikt til å beskytte skjermingsverdige objekter*
Forskrift om objektsikkerhet § 3-1 *– Generelle krav til beskyttelsen*
Forskrift om sikkerhetsadministrasjon kapittel 4 *– Risikohåndtering og sikkerhetsrevisjon*

Det generelle kravet til sikringen av skjermingsverdige objekt er altså at tap og skade skal avverges eller begrenses. Ut over disse formålene gir ikke objektsikkerhetsforskriften konkrete føringer for **hvordan** eller **hvor godt**, foruten at tiltakene skal bestå av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon. Så hvordan skal virksomheten kunne avgjøre når sikringen er god nok?

Objektsikkerhetsforskriften viser her til forskrift om sikkerhetsadministrasjon, og dennes bestemmelser om risikohåndtering, risikovurdering, sikkerhetsrevisjon og ledelsens evaluering.

Heller ikke i disse bestemmelsene gis det konkrete føringer for avdømming av hva som kan anses tilstrekkelig sikkert, eller hvordan vurderingen skal dokumenteres. Det er likevel klart at det må gjennomføres en risikoanalyse i en eller annen form. Det eksisterer ulike modeller med forskjellig tilnærming og detaljeringsnivå, og som passer til ulike objekttyper.

NSM vil normalt ikke pålegge bruk av en spesifikk type analysemodell, men objekteier kan selv velge den metoden som best egner seg for det aktuelle objektet. For at intensjonen i bestemmelsene om risikohåndtering skal kunne sies å være oppfylt må imidlertid et minste minimum av faktorer belyses og dokumenteres.

- Hva skal sikres?
  - Gjennom skadevurderingen skal virksomheten ha identifisert hvilke objekter som må skjermes.
- Hva skal det sikres mot?
  - Sikringstiltakene må uformes med sikte på trusselaktører med betydelig kapasitet.
- Hva skal sikringen oppnå?
  - Sikkerhetsloven angir funksjonelle krav for hver av de tre objektklassene. Dette er minimumskrav og må sees i forhold til den dimensjonerende trusselen.

8.1 Forslag til løsning

Nasjonal sikkerhetsmyndighet har utarbeidet en sjekkliste i stikkords form som kan benyttes i arbeidet.

Dette arbeidet begynner etter at man har gjennomført en verdivurdering med funksjonalitet i fokus.

Sikringsprosessen kan deles inn i fem hoveddeler:

1. Beskrivelse av objektet

2. Identifisering av sikringsmål
3. Definering av basistrussel
4. Design av sikringssystem
5. Evaluering

1. Objektbeskrivelse

Som tidligere nevnt i veilederen, bør man ikke begynne med objektet i seg selv, men med virksomhetens funksjon. Når kritikaliteten i denne er identifisert, vil man begynne beskrivelsen av objektet som skal sikres. Forhold som kan omtales er eksemplifisert nedenfor. Denne prosessen må ikke nødvendigvis være særlig strukturert eller bundet til de foreslåtte eksemplene. Beskrivelsen kan gjøres ved hjelp av prosa, tegninger, foto, diagrammer med mer. Nødvendig omfang avhenger av hvorvidt utenforstående skal delta i arbeidet.

Hensikten med beskrivelsen er å forstå objektet og omgivelsene for lettere å kunne identifisere sårbarheter og brukbare sikringsmekanismer.

- Fysiske forhold
  - Grenser
  - Bygninger
  - Rom
  - Adkomstveier og innganger
  - Infrastruktur – varme, ventilasjon, kommunikasjon, strøm
  - Bakgrunnsstøy, vibrasjoner, klima-/værforhold
  - Eksisterende sikring
  - Verifiser tegninger og beskrivelser
- Virksomheten
  - Produkt / leveranser
  - Ansatte – type, antall
  - Arbeidstider
  - Støttefunksjoner – anskaffelser, vedlikehold
  - Involvering og lokalisering av sjefer
- Prosedyrer
  - Prosess-/flytdiagrammer m.m.
  - Verifiser liv vs. lære
- Safety hensyn
- Lovhensyn og annet regelverk
  - Sektorregelverk
  - Personvern / Datatilsynet
  - Forsikring
  - Byggeforskrifter
  - Krav ang. bevegelseshemmede
  - Fagforeningsavtaler
- Lokalt politi
  - Tilgjengelighet
  - Avtaler

2. Målidentifisering

Ved å gå gjennom en prosess med å konkretisere sikringsmålene er det også mulig å fange opp andre objekter og funksjoner som er av kritisk betydning.

Hensikten med beskrivelsen er å bevisstgjøre helt klart hva det er som skal sikres og hva slags hendelser som er uønsket.

- Hva er det jeg har som trenger beskyttelse? Tekniske verdier / maskinpark, en funksjon som utføres i bygget, bygget i seg selv, ansatte og besøkendes liv og helse, viktige støttefunksjoner?
- Er det ulike driftsomstendigheter som må vurderes?
- Hvordan er IT-sikkerheten knyttet opp mot fysisk sikkerhet?
- Hvor – spesifikt – er målet lokalisert?
- Hva er målet verd for meg - konsekvens ved tap? Dette sier noe om hvilken risiko jeg er villig til å løpe.
- Hva er målet verd for de som er interessert i tyveri, skadeverk eller ødeleggelse? Dette sier noe om hvor langt en motstander er villig til å gå.
- Identifiser sikringsbehov
    - Tyveri fra lager
    - Tyveri fra prosess
    - Sabotasje, ødeleggelse
- Identifiser objekter
    - Materialiser funksjoner
    - Vitale støttesystem
- Identifiser målkategori (hvis ønskelig med verdidifferensiering / prioritetsrekkefølge)
    - Klassifiseringsgrad objekt
    - Klassifiseringsgrad følgeskade
- Lag målliste
    - List mål
    - List klassifiseringsgrad
    - List mållokalisering

Eksempel på enkel målliste:

Mål	Klass. / Kategori	Tyveri / Sabotasje	Lokalisering	Merknader

3. Trusseldefinering

Denne prosessen skal munne ut i en basistrussel – det vil si den trussel som er dimensjonerende for design av grunnsikringen og påbygningstiltak. Basistrusselen bør være så konkret som mulig og det bør listes hvilke intensjoner og kapasiteter sikringssystemet skal kunne motstå.

For skjermingsverdige objekt må man legge til grunn at mulige trusselaktører er fremmede makter eller internasjonale terrororganisasjoner som har en betydelig kapasitet. Når det gjelder hvilken type trusselaktør det er relevant å beskytte seg mot i henholdsvis grunnsikringen og beredskapsystemet, vises det til veiledningens beskrivelse av dimensjonerende trusselaktør. Mulig kapasitet til en slik trusselaktør innebærer at man må forutsette at denne trusselaktøren har oversikt over virksomhetens sårbarheter. Trusselaktøren vet hvor minst mulig innsats vil gi størst mulig effekt ved sikkerhetstruende virksomhet.

Uten en gjennomarbeidet og realistisk basistrussel er det en tung oppgave å vurdere om systemet er ”godt nok”. Alternativt kan sikringen også bli unødig ressurskrevende. Nedenfor er et eksempel på hvordan prosessen kan forløpe.

- Trusselvurdering
    - Politiets (Kripos, PST, lokalt PD) og andres vurdering av trusselbildet på kort og lang sikt.
    - Forutsett imidlertid at trusselsituasjonen endrer seg fortløpende. Objektsikkerhetsforskriften tar utgangspunkt i en normalsituasjon. Terrorisme, sabotasje og spionasje er i sin natur trusler man ikke kan forvente et forvarsel mot.
- Avklar forutsetninger, eksempelvis
    - Demonstrert vs. potensiell adferd
    - Troverdig vs. ”utrolig” trussel
    - Forvarsel eller ikke
    - Lokal, nasjonal eller internasjonal trussel
- Idédugnad i egen organisasjon
    - For et eksempel på skjema for brainstorming, se vedlegg C.
- Konkretiser og basistrusselen(e)
    - Noen trusler er svært ressurskrevende å sikre mot, spesielt uten forvarsel. De kan imidlertid ikke uten videre oversees av den grunn. Vær rasjonell og bevisst valgene som tas - også de trusler man velger ikke å sikre mot. Diskuter frem til enighet om basistrusselen og dokumenter denne. Listen over er ikke nødvendigvis uttømmende for momenter som kan være med.
    - Definer trusler som overstiger de systemet skal motstå. Disse må eventuelt håndteres ved påbygningstiltak for etter forhåndsvarsel. Sørg for planverk og avtaler.
    - Det kan være ulike trusler mot de forskjellige målene.
    - Kvalitetssikre med en sjekk mot de avklarte forutsetningene.

4. Design av sikringssystemet

Det er viktig å merke seg at ingen sikringstiltak er helt sikre. Det finnes ingen barrierer som ikke kan forseres eller omgås på en eller annen måte. Det bør derfor sikres i dybden – med mulighet for deteksjon og tidsforsinkelse i flere ledd.

Det bør også tilstrebes en god balanse i tiltakene. Med dette menes at det er tilnærmet lik tidsforsinkelse og deteksjonssannsynlighet i de ulike veiene en motstander kan velge frem til målet.

Denne veilederen går ikke i detalj på typer og kvaliteter på ulike sikringsmidler. Viktigere enn å fokusere på enkelttiltak er det å se helheten i et sikringssystem når det planlegges. Nedenfor er en liste stikkord for grunnleggende god design:

- **Deteksjon**
  - Tidligst mulig.
    - Deteksjon før en tidsforsinkende barriere teller mye mer enn etter.
  - Ulike typer.
    - Bruk av forskjellige sensortyper vanskeliggjør manipulering og omgåelse.
    - Mulighet for deteksjon før hver tidsforsinkende barriere.
    - Alt kan detekteres. Tenk gjennom hvilke handlinger eller hva slags opptreden eller uønsket tilstedeværelse du vil ha tidlig varsel om.
  - Deteksjon må evalueres / verifiseres.
    - Det er stor forskjell på å vite at noe skjer kontra å vite hva som skjer. En deteksjon uten verifikasjon utløser aldri en adekvat reaksjon.

- **Alarmoverføring**
  - Sannsynligheten for reaksjon avgrenses av sannsynligheten for alarmoverføring. Det bør derfor ikke spares her.
  - Flere overføringsveier.
    - Overføring av alarmer bør være mulig på flere måter.
    - Alarmlinjene bør overvåkes.
  - Herding av vakt.
    - Vakter bør alltid være sikret slik at de kan utføre primærfunksjonen varsling i nærvær av basistrusselen.

- **Forsinkelse**
  - Barrierer i flere ledd av økende styrke mot målet.
  - Materialkombinasjoner.
    - Tidsforsinkende barrierer bør konstrueres av ulike materialer slik at en inntrenger må benytte flere verktøystyper for å trenge gjennom.
  - Forsinkelse før deteksjon teller ikke.
    - En tidsforsinkende barriere uten deteksjon i forkant har liten verdi.

- **Reaksjon**
  - ”Tilstrekkelig i tide”.
  - Merk sabotasje versus tyveri (krav til tid)
  - Merk avverge versus begrense skade (krav til styrke)

Deteksjon og forsinkelser i flere ledd med tilstrekkelig reaksjon i tide. Disse grunnleggende tiltakene i kategoriene over hører naturlig sammen i en kjede. Dersom kjeden ikke er komplett, eller ett sett med tiltak ikke er til stede, forringes verdien av de andre dramatisk. Det spiller eksempelvis ingen rolle hvor sterk en vegg er dersom forsøk på inntrenging ikke oppdages. Forsøket vil lykkes.

I tillegg til å fokusere på et sikringssystem som har balanse i tiltakene ovenfor kan det være nyttig se på noen andre forhold ved design av forebyggende sikring.

- Tiltak som kan bidra til avskrekking kan være:
  - Synlige barrierer og kontrolltiltak.
  - Skilting og annet varsel.
  - Åpen og ryddig sone for mottak av publikum.
  - Tillitvekkende sikkerhetsopptreden.

- Tiltak som kan bidra til at et angrep avbrytes kan være:
  - Ikke varslede eller synlige deteksjonsmekanismer.
  - Alarm og varsling som tiltrekker generell oppmerksomhet.
  - Skjulte forsterkninger eller barrierer som ikke er synlig for publikum.
  - Barrierer som utløses ved alarm.

- Tiltak mot en i norsk sammenheng sjelden, men i særstilling alvorlig, trussel; eksplosjoner.
  - Tiltak for å holde avstand til en eksplosjon; hver eneste meter teller.
  - Materialvalg og tiltak for å redusere spredning av fragmenter / splinter.

5. Evaluering

Det er i de foregående stegene nå helt klart definert **hva** som skal beskyttes og **hvem** det skal beskyttes mot. En evaluering av den foreslåtte sikringsplanen kan nå gjøres.

Selvsagt vil det komme til problemstillinger omkring grad av måloppnåelse, sannsynlighet for deteksjon, og hva som kan anses som tilstrekkelig reaksjon i tide. Det finnes evalueringsverktøy for denne type av sannsynlighetsberegning og risikomåling. Slike kan oppleves som for kompliserte til at en hvilken som helst virksomhet skal kunne benytte dem. Som et minimum må imidlertid enhver evaluering dokumenteres på en eller annen måte. Dette for å kunne ta beslutninger basert på etterprøvbare fakta, samt å få et bevisst forhold til restrisiko.

En evaluering bør minimum inneholde:

- Dokumentert basistrussel.
- Prinsippskisse eller bygningstegning med de foreslåtte sikringstiltakene inntegnet.
  - Marker mål som skal sikres.
  - Marker inntrengningsveier mot målet som gir basistrusselen minst sannsynlighet for å bli detektert.
  - Marker deretter inntrengningsveier som gir basistrusselen raskest vei til målet.
- Dersom basistrusselens “stilleste” og “raskeste” vei til målet er akseptable ut i fra forventet reaksjon, dokumenter dette, eventuelt gjør endringer i designen.
- Kontroll av at tiltak ikke enkelt kan settes ut av spill av en utro tjener.

Vedlegg A

LOV OG FORSKRIFT OM OBJEKTSIKKERHET

Klikk på teksten for link til Lovdata (www.lovdata.no).

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) kapittel 1: Alminnelige bestemmelser

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) kapittel 5: Objektsikkerhet.

Forskrift om objektsikkerhet.

Vedlegg B

SKADEVURDERING I PRAKSIS[15]

Et forslag til en praktisk, forenklet skadevurdering presenteres i det følgende. Skadevurderingene danner grunnlag for departementenes utpeking og klassifisering av skjermingsverdige objekter.

At alt ikke er like vesentlig å sikre er et enkelt, men fundamentalt, utgangspunkt for all sikkerhetstenkning. Viktige verdier må beskyttes best, ut i fra en skadevurdering av negative konsekvenser for en eller flere verdier dersom uønskede hendelser skjer.

Skadevurdering er en viktig del av forebyggende sikkerhetsarbeid, og en integrert del av opprettholdelsen av rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Rikets sikkerhet endres i takt med samfunnsutviklingen, og tverrsektorielle avhengigheter gjør forsvar av Riket til mer enn et militært anliggende.

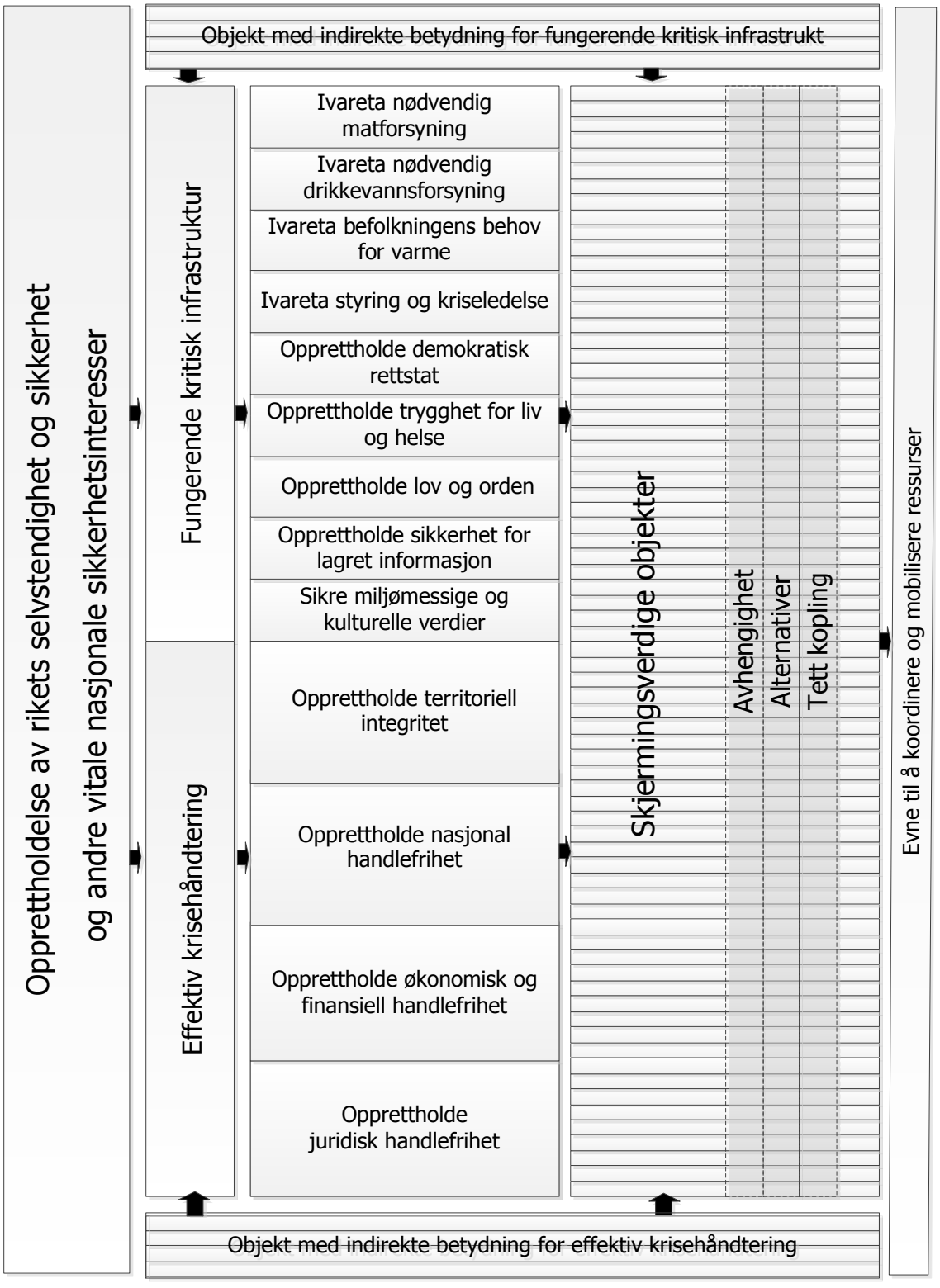
Noen objekter kan utgjøre fare eller ha en sterk symbolverdi. Disse kan ha en indirekte betydning for Rikets selvstendighet og sikkerhet. Samtidig er det slik at objekter i seg selv ikke er skjermingsverdige. Det er den sikkerhets*funksjonen* objektet har eller understøtter som gjør det skjermingsverdig. Eksempelvis er det er lite trolig at et sykehus i sin helhet er et skjermingsverdig objekt. Spesielle sykehusfunksjoner kan derimot være kritiske. Fasiliteter nødvendige for å opprettholde slike funksjoner er i så fall skjermingsverdige.

Dette vedlegget er ment som et verktøy for å gjennomføre en skadevurdering. Dette innebærer at det er et hjelpemiddel og ikke en fasit på gjennomføring. Utgangspunktet for denne modellen er opprettholdelse av rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. For å kunne bringe dette begrepet nærmere et gripbart objekt, søker steg 1 (se illustrasjon) å ta for seg et mulig skjermingsverdig objekts indirekte evne til å påvirke kritisk infrastruktur eller effektiv krisehåndtering, ut fra en normaltilstand. Fra vurderingskriteriene nedfelt i sikkerhetslovens § 17, kan man deretter bryte ned delfunksjonene som steg 2 til 4 foreslår for å vurdere skadefølger ved bortfall av virksomhetens leveranse og funksjon som mulig skjermingsverdig objekt.

[15] Dr. Morten Bremer Mærlie, DNV

STEG 1Hovedmålsetning

Opprettholdelse av rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.



Figur B1 Skadevurderingsprosess og tilhørende elementer

STEG 2A. Effektiv sikkerhetspolitisk krisehåndtering

Kan en eventuell ødeleggelse, nedsatt funksjonalitet eller rettstridig overtakelse av objektet ha betydning for evnen til å (*kryss av*):

- ☐ 1. opprettholde territoriell integritet?
- ☐ 2. opprettholde konstitusjonell handlefrihet?
- ☐ 3. opprettholde økonomisk og finansiell handlefrihet?
- ☐ 4. opprettholde juridisk handlefrihet?

For identifiserte punkter, fyll inn Tabell 2A (tabellen utvides ved behov).

STEG	EFFEKTIV KRISEHÅNDTERING	SKJERMINGSVERDIG OBJEKT	OBJEKTEIER
2A.1	Territoriell integritet		
2A.2	Konstitusjonell handlefrihet		
2A.3	Økonomisk og finansiell handlefrihet		
2A.4	Juridisk handlefrihet		

STEG 2B. Fungerende kritisk infrastruktur

Kan en eventuell ødeleggelse, nedsatt funksjonalitet eller rettstridig overtakelse av objektet ha betydning for evnen til å (*kryss av*):[16]

- ☐ 1. Ivareta nødvendig matforsyning?
- ☐ 2. Ivareta nødvendig drikkevannsforsyning?
- ☐ 3. Ivareta befolkningens behov for varme?
- ☐ 4. Ivareta styring og kriseledelse?
- ☐ 5. Opprettholde demokratisk rettstat?
- ☐ 6. Opprettholde trygghet for liv og helse?
- ☐ 7. Opprettholde lov og orden?
- ☐ 8. Opprettholde sikkerhet for lagret informasjon?
- ☐ 9. Sikre miljømessige og kulturelle verdier?

For identifiserte punkter, fyll inn Tabell 2B (tabellen utvides ved behov).

STEG	FUNGERENDE KRITISK INFRASTRUKTUR	SKJERMINGSVERDIG OBJEKT	OBJEKTEIER
2B.1	Nødvendig matforsyning		
2B.2	Nødvendig drikkevannsforsyning		
2B.3	Befolkningens behov for varme		
2B.4	Styring og kriseledelse		

[16] Direktoratet for samfunnssikkerhet og beredskap 2012, Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring, s. 25

2B.5	Demokratisk rettsstat		
2B.6	Trygghet for liv og helse		
2B.7	Lov og orden		
2B.8	Sikkerhet for lagret informasjon		
2B.1	Miljømessige og kulturelle verdier		

STEG 3A. Forsterkende symboleffekter

Kan hendelser mot dette objektet medføre endringer i befolkningsadferd (symbolmål), i så stor grad at dette kan ha betydning for

- 1. effektiv sikkerhetspolitisk krisehåndtering?
- 2. fungerende kritisk infrastruktur?

For identifiserte punkter, fyll inn Tabell 3A (tabellen utvides ved behov).

STEG	OBJEKT AV BETYDNING FOR	SKJERMINGSVERDIG OBJEKT	OBJEKTEIER
	Sikkerhetspolitisk krisehåndtering		
2A.1	Territoriell integritet		
2A.2	Konstitusjonell handlefrihet		
2A.3	Økonomisk og finansiell handlefrihet		
2A.4	Juridisk handlefrihet		
	Kritisk infrastruktur		
2B.1	Nødvendig matforsyning		
2B.2	Nødvendig drikkevannsforsyning		
2B.3	Befolkningens behov for varme		
2B.4	Styring og kriseledelse		
2B.5	Demokratisk rettsstat		

2B.6	Trygghet for liv og helse		
2B.7	Lov og orden		
2B.8	Sikkerhet for lagret informasjon		
2B.1	Miljømessige og kulturelle verdier		

STEG 3B. Forsterkende fareeffekter

Kan hendelser mot objektet utgjøre en fare for miljøet eller befolkningens liv og helse, i så stor grad at dette kan ha betydning for

- ☐ 1. effektiv sikkerhetspolitisk krisehåndtering? *Hvis Ja, gå til STEG 2A*
- ☐ 2. fungerende kritisk infrastruktur? *Hvis Ja, gå til STEG 2B*

For identifiserte punkter, fyll inn Tabell 3B (tabellen utvides ved behov).

STEG	OBJEKT AV BETYDNING FOR	SKJERMINGSVERDIG OBJEKT	OBJEKTEIER
	Sikkerhetspolitisk krisehåndtering		
2A.1	Territoriell integritet		
2A.2	Konstitusjonell handlefrihet		
2A.3	Økonomisk og finansiell handlefrihet		
2A.4	Juridisk handlefrihet		
	Kritisk infrastruktur		
2B.1	Nødvendig matforsyning		
2B.2	Nødvendig drikkevannsforsyning		
2B.3	Befolkningens behov for varme		
2B.4	Styring og kriseledelse		
2B.5	Demokratisk rettsstat		

2B.6	Trygghet for liv og helse		
2B.7	Lov og orden		
2B.8	Sikkerhet for lagret informasjon		
2B.1	Miljømessige og kulturelle verdier		

STEG 4 Koordinering og mobilisering av ressurser

Koordinering og mobilisering av ressurser kan være avgjørende for opprettholdelse av rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. I forkant av eventuelle kriser, fordrer dette vurdering av skjermingsverdige objekters innbyrdes relasjoner. Sektorer og departementenes underliggende etater kan ha særskilte oppgaver i denne sammenheng.[17]

a. Avhengighet

Bortfall av infrastruktur som et stort antall er avhengig av har alvorlige konsekvenser, og dette kriteriet veier tyngst når kritisk infrastruktur skal identifiseres. Eksempelvis er hele samfunnet avhengig av en veginfrastruktur for å fungere. På samme måte er praktisk talt alle samfunnsfunksjoner avhengig av strøm gjennom kraftinfrastrukturen og vann gjennom vannforsyningsinfrastrukturen.

b. Alternativer

Manglende alternativer tilsier kritikalitet. Eksempelvis har Norge et stort antall kraftverk spredt ut over hele landet. Dette medfører at bortfall av ett kraftproduserende anlegg ikke får store konsekvenser for kraftleveransen sett under ett. Dette står i motsetning til land med noen få, men store kraftproduserende enheter. Bortfall av ett kraftproduserende anlegg vil i slike tilfeller få store konsekvenser på grunn av manglende alternativer av kraftproduserende enheter.

c. Tett kobling

Et tett koblet system innebærer at forstyrrelser ett sted i systemet får umiddelbare konsekvenser for systemet som helhet. Mestring av et tett koblet system krever sentralisert styring. Høy grad av tett kobling tilsier kritikalitet. Eksempler kan hentes fra offentlig transport. Jernbane og lufttrafikk i Norge er avhengig av sentralisert styring i sanntid for effektiv og sikker drift. Busstrafikk kan derimot operere uten en sentralisert styring, eller i hvert fall med langt lavere grad av sentralisert kontroll og styring i sanntid. Bortfall av knutepunkter i tett koblede systemer vil få store konsekvenser for funksjonsdyktigheten til infrastrukturen. El-nettet, særlig sentralnettet, er et ytterligere eksempel.

Vedlegg C

IDESKJEMA TRUSSELDEFINERING

Ref kapittel 8.

[17] Den følgende teksten er i sin helhet hentet fra NOU 2006: 6. «Når sikkerheten er viktigst», para. 3.1

* = Lav, Medium, Høy	**Demonstrant**	**Kriminell**	**Terrorist**	**Psykotisk person**	**Sabotør**
Hensikt					
Tyveri					
Ødeleggelse					
Annet _____					
Motivasjon					
Ideologisk					
Økonomisk					
Personlig					
Kapasitet					
Antall					
Våpen					
Eksplosiver					
Kjøretøy					
Verktøy					
Tekniske ferdigheter					
Økonomi					
Infrastruktur/støtte					
Samarbeid med insider					
Adgangsrettigheter					
Privilegier					
Kunnskap					
Passiv / aktiv					
Voldelig / ikkevold					
Rasjonell / irrasjonell					

Sikkerhet er først og fremst en prosess, ikke en endelig tilstand. Trusler vil endre seg i karakter – det er grunnsikring som er i forkant av uønskede hendelser.