Nasjonal sikkerhetsmyndighet

**Veiledning**

Sist oppdatert: 2009-04-14

# Veiledning i verdivurdering

Dette er et grunnleggende prinsipp i vårt demokrati å tilstrebe mest mulig åpenhet i forvaltningen, og i utgangspunktet skal all informasjon være offentlig tilgjengelig. Samtidig vil det til enhver tid være informasjon og objekter som er sensitive og har et beskyttelsesbehov. Dette er informasjon og objekter som er så viktige av hensyn til rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser at de må skjermes i henhold til kravene i sikkerhetsloven.

Denne veiledningen søker å bidra til å identifisere hva som bør skjermes.

# 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.

## Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

**Postadresse**
Postboks 14
1306 BÆRUM
POSTTERMINAL

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

**Militær telefon/telefaks**
515 40 00/515 40 09

**Internettadresse**
www.nsm.stat.no

# Innholdsfortegnelse

# 1 Hvorfor verdivurdering?

Forebyggende sikkerhetstenkning begynner med verdivurdering. Målgruppen for denne veiledningen er derfor primært virksomheter, det være seg offentlige eller private, som er underlagt sikkerhetsloven[1]. Men også andre virksomheter som behandler sensitiv informasjon eller råder over kritiske objekter vil ha nytte av veiledningen. Hensikten med veiledningen er å gi virksomhetene et hjelpemiddel til å identifisere hva som er skjermingsverdig informasjon[2] og skjermingsverdig objekt[3], og i hvilken grad de er skjermingsverdige, for å finne frem til riktig grad av beskyttelsestiltak.

Det er et grunnleggende prinsipp i vårt demokrati å tilstrebe mest mulig åpenhet i forvaltningen, og i utgangspunktet skal all informasjon være offentlig tilgjengelig[4]. Samtidig vil det til enhver tid være informasjon og objekter som er sensitive og som har et beskyttelsesbehov.

Det er en målsetting at denne veiledningen kan gi inspirasjon til å tenke verdivurdering når informasjon tilvirkes. Det er eieren av informasjonen eller objektet som selv må foreta en verdivurdering og fastsette riktig graderingsnivå.

Denne veiledningen er ment å være en overordnet veiledning. De enkelte sektorer vil av ulike årsaker ha mer spesifikke tilnærminger til verdivurdering. NSM anbefaler at hver enkelt sektor selv utarbeider slike veiledninger.

## 1.1 Grunnleggende begreper i sikkerhetsloven

Sikkerhetsloven er utformet blant annet med den hensikt å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og vitale nasjonale sikkerhetsinteresser. I kapittel 2 vil det gjøres rede for hva man legger i disse overordnede begrepene.

Etter sikkerhetslovens § 11annet ledd skal den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon, sørge for at informasjonen merkes med aktuell sikkerhetsgrad. Etter sikkerhetslovens § 12 er det plikt til å beskytte sikkerhetsgradert informasjon for å hindre at uvedkommende får kjennskap til informasjonen.

Med skjermingsverdig informasjon menes informasjon som er av betydning for rikets eller alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale interesser, dersom det kan medføre skade om informasjonen blir kjent av uvedkommende.

De sikringstiltakene sikkerhetsloven angir gjennomføres for alt og alle i forebyggende hensikt og uavhengig av konkrete mistanker om sikkerhetstrusler.

Sikringstiltak er all planlegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av forberedelse til, forsøk på eller gjennomføring av spionasje, sabotasje eller terrorhandlinger.

Et annet grunnleggende begrep er det som kalles *sikkerhetstruende hendelser*[5]. Dette inkluderer sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.

*Sikkerhetstruende virksomhet;* forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet.

*Kompromittering:* tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon, herunder uønsket avhending, modifisering eller ødeleggelse.

---

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

[2] Skjermingsverdig informasjon: Informasjon som skal merkes med sikkerhetsgradering i henhold til lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) § 11. Det skilles mellom sikkerhetsgradene STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT og BEGRENSET. Se forøvrig vedlegg A.1. for oversikt over begreper og terminologi

[3] Skjermingsverdig objekt: Eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale, nasjonale sikkerhetsinteresser, jf sikkerhetsloven § 3 pkt 12.

[4] Jf offentleglova av 19. mai 2006 nr. 16 § 1

[5] Jf forskrift om sikkerhetsadministrasjon § 1-2 pkt 3

*Sikkerhetsbrudd* er brudd på bestemmelse om sikkerhetstiltak gitt i sikkerhetsloven eller forskrifter til sikkerhetsloven.

## 1.2 Verdivurderingens plass i forebyggende sikkerhetsarbeid

Det mest fundamentale med sikkerhet er forutsetningen om at man har noe – en verdi – som man ønsker å beskytte. Dette kan være økonomiske verdier som ens egne penger, en virksomhets aktiva eller samfunnets samlede verdier. Det kan også tenkes annet som er verd å beskytte, som for eksempel muligheten til å bevege seg i naturen, kvaliteten på vann og mat, retten til å mene og ytre seg om hva man vil, friheten til å selv kunne være med på å velge hvem som skal styre landet, retten til å praktisere sin egen religion, frihet fra kriminalitet, en sunn helse eller fravær av krig.

Verdiene som ønskes opprettholdt kan altså være av materiell eller ikke materiell art.

Forebyggende sikkerhetsarbeid bygger på følgende forutsetninger:

- En rasjonelt tenkende *aktør* som gjennomfører sikkerhetsmessige vurderinger
- *En verdi eller flere verdier* som aktøren ønsker ivaretatt eller opprettholdt, ut fra tanken om at det er *skadelig* dersom verdiene blir redusert eller tapt
- En antatt intern eller ekstern *trussel* eller *trusselaktør*
- Kunnskap om verdienes *sårbarhet/motstandsdyktighet*
- Gjennomførbare *tiltak* for å avverge trusselen eller håndtere konsekvensene dersom den inntreffer, slik at skade ikke oppstår eller at den i hvert fall reduseres så mye som mulig
- *Rammefaktorer* som vil fremme eller hemme aktørens evne eller vilje til å gjennomføre tiltak

En fundamental tanke innen forebyggende sikkerhetsarbeid er at ikke alt er like vesentlig å beskytte. Dette innebærer at man må utvikle systemer for ikke bare å kunne identifisere hva som har sikkerhetsmessig verdi, men også kunne klassifisere det i forhold til andre sammenlignbare verdier. De to andre fundamentale komponentene vil være det til enhver tid gjeldende trusselbilde samt oversikt over sårbarheter. Disse to siste komponentene vil ikke bli behandlet i denne veiledningen.

## 1.3 Hva sier sikkerhetsloven om verdivurdering?

Begrepet *verdivurdering* er ikke definert i loven, og benyttes heller ikke i lovtekst eller eksisterende forskrifter. For å kunne oppfylle lovens bestemmelse, må det foretas vurderinger som vil danne grunnlag for å identifisere skjermingsverdig informasjon og skjermingsverdige objekter.

Verdivurdering i forhold til sikkerhetsloven kan dermed defineres på følgende måte:

> **En analyse som har til hensikt å identifisere hvilke objekter og hvilken type informasjon som er så viktige av hensyn til rikets sikkerhet og vitale nasjonale sikkerhetsinteresser at de må skjermes.**

Utgangspunktet er en systematisk tankegang om hvilke skadefølger det vil kunne få dersom informasjonen eller objektene rammes av sikkerhetstruende hendelser.[6]

[6] Sikkerhetstruende hendelse: Sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd. Sikkerhetstruende virksomhet: Forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandliner, samt medvirkning til slik virksomhet, jf sikkerhetsloven § 3 pkt 2. Kompromittering: Tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon, herunder uønsket avhending, modifisering eller ødeleggelse. Forskrift om sikkerhetsadministrasjon § 1-2 pkt 3.

## 1.4 Hvem har ansvar for å foreta verdivurdering?

Det er virksomheten[7] selv som må forestå verdivurdering. Den som utsteder informasjon skal på forhånd vurdere omfanget av eventuelt skadepotensiale dersom uvedkommende får tilgang til informasjonen, og ut fra denne vurderingen sikkerhetsgradere den.[8]

Informasjonseier eller utsteder av informasjon er det samme som en virksomhet. I denne sammenheng er virksomhet tilsvarende med et forvaltningsorgan eller annet, det være seg offentlige eller private som *faller inn under sikkerhetslovens virkeområde*. Ansvaret for verdivurdering tilligger etter linjeorganisasjonsprinsippet virksomhetens leder.

Identifisert skjermingsverdig informasjon må defineres inn i riktig graderingsnivå.

## 1.5 Merking av sikkerhetsgradert informasjon

Sikkerhetsgradering innebærer at den som utsteder eller på annen måte tilvirker skjermingsverdig informasjon skal sørge for at informasjonen merkes med aktuell sikkerhetsgrad.[9] Informasjonen må påføres graderingsmerke for å synliggjøre de tiltak som sikkerhetsloven pålegger for å skjerme informasjonen. Mottaker av sikkerhetsgradert informasjon er forpliktet til å respektere den graderingen som er gjort av utsteder.[10]

[7] Et forvaltningsorgan eller annet rettssubjekt som sikkerhetsloven er gjort gjeldende for, jf sikkerhetsloven § 2

[8] Forskrift om informasjonssikkerhet § 2-1, *Skadevurdering*

[9] Sikkerhetsloven § 11, *Sikkerhetsgradering*

[10] Se NSMs veiledning i informasjonssikkerhet (merking av sikkerhetsgradert informasjon og informasjonssystemer)

# 2 Begrepene ”rikets selvstendighet og sikkerhet” og ”andre vitale nasjonale sikkerhetsinteresser”

## 2.1 ”Rikets selvstendighet og sikkerhet”

Den forebyggende sikkerhetstjeneste skal i henhold til sikkerhetsloven legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. I forarbeidene til sikkerhetsloven har dette tradisjonelt vært nært knyttet til det militære forsvaret av territoriet, samt alliansetilknytningen. Det presiseres at med ”rikets sikkerhet” både siktes til indre og ytre sikkerhet.[11]

Straffelovkommisjonen utredet og drøftet i 2003[12] det nærmere innholdet av ”rikets sikkerhet”. Dette begrepet er brukt i en rekke forskjellige lover. Kommisjonen understreket at innholdet i begrepet ikke er helt klarlagt, og at det ikke nødvendigvis har den samme betydning i samtlige bestemmelser som kommisjonen har vurdert. Imidlertid pekes det på at det har skjedd en endring i tidens løp. Når det gjelder åpenbaring av noe som bør holdes hemmelig av hensyn til rikets sikkerhet, var det tidligere et vilkår i straffebestemmelsene at det dreide seg om opplysninger som måtte holdes hemmelige av hensyn til rikets sikkerhet ”lige ovenfor anden stat”. De rammet altså ikke hemmelighold i forhold til andre enn stater, eksempelvis terroristgrupper og ekstremistiske organisasjoner. Ved lovendring 3 desember 1999 nr. 82 ble begrensningen fjernet. I forarbeidene til den nevnte lovendring sies bl a:

> ”*Eksempler på slike opplysninger kan være opplysninger omkring beredskaps- og sikkerhetsopplegg, omkring statsbesøk, begivenheter i kongehuset og andre nasjonale arrangementer. Det kan tenkes at det vil være skadelig av hensyn til rikets sikkerhet at slike opplysninger åpenbares, for eksempel til en terroristorganisasjon, selv om det ikke vil ha den samme skadelige virkningen som om en fremmed stat fikk opplysningen.*”[13]

Det synes klart at nasjonal handlefrihet og integritet må komme inn under *rikets sikkerhet*. Nasjonal handlefrihet og integritet kan brytes ned til underpunkter:

- konstitusjonell handlefrihet
- økonomisk og finansiell handlefrihet
- juridisk handlefrihet
- sikkerhetspolitisk handlefrihet
- innenriks- og utenrikspolitisk handlefrihet
- territoriell integritet

Oversikten er ikke uttømmende.

## 2.2 ”Andre vitale nasjonale sikkerhetsinteresser”

Verdivurdering skal også gjøres i forhold til i hvilken grad ”andre vitale nasjonale sikkerhetsinteresser” kan bli skadelidende. Dette begrepet ble først introdusert da sikkerhetsloven ble vedtatt. Det var en intensjon om å bli kvitt den tidligere skjønnsmessige formuleringen om å gradere ”opplysninger av sikkerhetsmessig verdi” som lå til grunn for dette. I lovens forarbeider sies at endringen for praktiske formål ikke skal innebære en utvidelse i forhold til tidligere vilkår for sikkerhetsgradering.

I forarbeidene heter det videre:

[11] Ot.prp. nr. 49 (1996-97), s.22 og 64

[12] NOU:2003:18 Rikets sikkerhet, Straffelovkommisjonens delutredning VIII

[13] Ot.prp. nr. 64 (1998-99), s. 142, (referert i NOU 2003:18)

> *"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. Det må legges til grunn at slike opplysninger etter dagens regler som den klare hovedregel vil kunne unntas fra offentlighet etter offentlighetslovens unntaksbestemmelser. Begrepet er likevel foreslått for å indikere at det kan være grunn til å skjerme informasjon etter loven, selv om informasjonen ikke har direkte sammenheng med rikets territorielle sikkerhet. Det vil for eksempel dreie seg om opplysninger som må skjermes for å forebygge alvorlige terrorhandlinger, selv om terrorhandlingene ikke utføres av eller for en fremmed makt eller lignende og således ikke nødvendigvis vil berøre riktets territorielle sikkerhet."*[14]

I Straffelovkommisjonens drøfting av begrepet "rikets sikkerhet" i forhold til spørsmålet om hva som skal vernes av straffeloven, bringes begrepet "grunnleggende nasjonale interesser" inn:

> *"Under en hver omstendighet finner utvalget at vernet om innhenting og avsløring av hemmelige opplysninger, ikke bør begrenses til interesser som gjelder rikets sikkerhet i tradisjonell forstand, men at også grunnleggende nasjonale interesser bør omfattes. Ved siden av forholdet til andre stater, herunder forhandlingsposisjoner, er det nærliggende å fremheve de interesser som er knyttet til:*
>
> - *infrastrukturen,*
> - *energi-, mat- og vannforsyning,*
> - *samferdsel og telekommunikasjon,*
> - *helseberedskap,*
> - *bank- og pengevesen*
> - *og andre samfunnsøkonomiske forhold.*[15]*. "*

I den grad innføringen av begrepet "vitale nasjonale sikkerhetsinteresser" i det hele tatt kan sees på som en utvidelse i forhold til tidligere regler, sies det i proposisjonen[16] at det vil kunne få som konsekvens at enkelte opplysninger som tidligere ble gradert etter Beskyttelsesinstruksen, i stedet skal behandles som skjermingsverdig informasjon og sikkerhetsgraderes etter sikkerhetsloven.

Innføringen av begrepet gir også mulighet for å beskytte informasjon som kan skade vitale nasjonale sikkerhetsinteresser, se også offentleglovas § 20 (unntak av hensyn til Norges utanrikspolitiske interesser) og § 21 (forsvars- og sikkerhetsinteresser) og § 23 (unntak av hensyn til det offentliges forhandlingsposisjon)[17].

Det vises til Infrastrukturutvalget[18] hvor utvalget viser til "nye" sikkerhetsutfordringer som terrorisme og konsekvenser og klimaendringer som berører samfunnet som helhet, og gir særskilte utfordringer for sikkerheten i virksomheter som har ansvar for kritisk infrastruktur og kritiske samfunnsfunksjoner.

Disse virksomhetene må ha evne til å håndtere både nye og gamle sikkerhetsutfordringer, enten disse skyldes utilsiktede eller tilsiktede handlinger.

En sentral oppgave for utvalget var å kartlegge virksomheter av betydning for rikets sikkerhet og vitale nasjonale interesser, det vil si kartlegge kritiske infrastrukturer og kritiske samfunnsfunksjoner.

Utvalgets definisjon av kritisk infrastruktur:

---

[14] Ot.prp. nr. 49 (1996-97), s.33

[15] NOU 2003:18, s. 72

[16] Ot.prp. nr. 49 (1996-97). s.34

[17] Offentleglova av 19. mai 2006 nr 16

[18] NOU 2006:6 – Når sikkerheten er viktigst, side 15 – Beskyttelse 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.

For å konkretisere begrepet kritisk infrastruktur, skiller utvalget mellom kritisk infrastruktur og kritiske samfunnsfunksjoner.

En presis tilnærming til hva kritisk infrastruktur er, innebærer å identifisere både kritisk infrastruktur og kritiske samfunnsfunksjoner:

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

Utvalget har ikke eksplisitt vurdert de kritiske samfunnsfunksjonene som står i kursiv. Med bakgrunn i dette arbeidet foreslo bl.a utvalget en lovendring i sikkerhetsloven som gjelder objektsikkerhet[19].

19 Lov av 11. april 2008 nr. 9 om endringer i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)

# 3 Verdivurdering og dens komponenter

Informasjonens kvalitetsmessige verdi er et produkt av at den er nøyaktig, relevant, tidsriktig, i en tilgjengelig form og mest mulig komplett. Informasjon fungerer som regel alltid i en kontekst, og gir mening når den tolkes sammen med kunnskap og erfaring hos dem som skal bruke den.

## 3.1 De tre sikkerhetsaspektene: konfidensialitet, integritet og tilgjengelighet

I sikkerhetsarbeidet er det vanlig å forholde seg til tre aspekter: *konfidensialitet, integritet og tilgjengelighet.*

Med *konfidensialitet* menes den egenskap at informasjonen ikke er tilgjengelig for uautorisert personell eller i ikke godkjente systemer.

Med *integritet* menes trygghet for at både informasjon forblir fullstendige, riktige og gyldige både i systemet og under forsendelse. Videre at informasjonen er konsistent og oppdatert.

Med *tilgjengelighet* forstås at informasjonen er tilgjengelig for de som skal bruke dem. Verdien av tilgjengelighet må konkretiseres gjennom krav til tilgjengelighet og respons.

Når det gjelder beskyttelse av informasjon av hensyn til rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser har det tradisjonelt vært fokusert mest på konfidensialitetsaspektet. I dag legges det stadig større vekt på sikring i forhold til tilgjengelighet og integritet. Ikke minst er dette viktige aspekt ved beskyttelse av skjermingsverdige objekter og kritisk infrastruktur.

## 3.2 Skadepotensialet

Et grunnleggende aspekt ved verdivurdering av informasjon og objekter er å vurdere hvilken skade som kan oppstå dersom informasjon kompromitteres eller et objekt settes ut av spill. Dette innebærer at man må forsøke å utlede konsekvenser i forhold til tap av konfidensialitet, tilgjengelighet eller integritet for informasjonen/objektet sett opp mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Vurderingstema i denne forbindelse vil være:

- I hvilken grad kan kompromittering av informasjon/ødeleggelse av objektet utnyttes av en ondsinnet trusselaktør?
- Hvilken alvorlighet kan skaden ha på rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser?
- Egen virksomhets operasjoner og beslutninger?
- Andres virksomhet og operasjoner?

## 3.3 Verdivurdering som del av risiko- og sårbarhetsanalyse

Risikovurdering innebærer bl.a. identifikasjon av virksomhetskritisk informasjon og objekter med tanke på å fastsette de riktige sikkerhetstiltakene både ut fra et "security" og et "safety" aspekt. Med security-aspekt menes her uønskede villede hendelser (f eks forsøk på sabotasje), mens safety-aspektet inkluderer uønskede hendelser (f eks naturkatastrofer). I prosessen med å utarbeide ROS-analyser[20] vil verdivurdering være en del av den analysen som må gjøres. Det er i denne sammenhengen et viktig moment at den enkelte virksomhet har evne til å kunne bedømme endringer i trussel- og risikobildet.

## 3.4 Tidsperspektivet

En grunnsikring innebærer en hensiktsmessig og betryggende skjermingspolitikk som tar inn over seg eksisterende trusler og sårbarheter samtidig som man også evner å se utover dagens risikobilde. Det innebærer at det må tas høyde for oppdukkende mulige endringer i et langsiktig perspektiv.

[20] For videre informasjon om ROS-analyser, se veiledning i ROS–analyse på NSMs hjemmeside: www.nsm.stat.no

## 3.5 Gjensidige avhengigheter

Det vil være et eget punkt i en verdivurdering å fastsette i hvilken grad konsekvensene av en sikkerhetstruende hendelse i eller mot egen virksomhet kan påføre *andre* virksomheter avgjørende skade. Likeledes må virksomheten/virksomhetens leder vurdere hvilke vitale skader virksomheten kan bli påført av en annen virksomhet hvis den sistnevnte rammes av en sikkerhetstruende hendelse. I denne sammenheng er det viktig å ha en oversikt over mulige gjensidige avhengigheter.

## 3.6 Graderingsnivåene for sikkerhetsgradert informasjon

Et sentralt spørsmål når det gjelder å vurdere om egen informasjon er skjermingsverdig i henhold til sikkerhetsloven, er om informasjonen kan misbrukes av uvedkommende (villede sikkerhetstruende hendelser) slik at det berører rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Sikkerhetsloven opererer med fire nivåer av alvorlighetsgrad når det gjelder potensiell skade ved kompromittering av skjermingsverdig informasjon:

> *STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
>
> *HEMMELIG nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
>
> *KONFIDENSIELT nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.*
>
> *BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.* [21]

Se også skjematisk oversikt over sikkerhetsloven, offentleglova og Beskyttelsesinstruksen i vedlegg A.3.

## 3.7 Fastsettelse av graderingsnivå

Den som utsteder informasjonen er den som på forhånd skal vurdere omfanget av en eventuelt skadepotensiale dersom uvedkommende skulle få tilgang til informasjonen. Derfor er det viktig at man finner et riktig graderingsnivå for informasjonen.

### 3.7.1 Overgradering eller overklassifisering

Ved overgradering av informasjon eller overklassifisering av objekt vil en effekt kunne være at færre får tilgang på informasjonen eller objektet enn de som bør ha tilgang på den. Et faremoment ved overgradering av informasjon kan videre være at graderingsnivået ikke respekteres. Et annet moment er at det påfører informasjonseier unødige administrative kostnader.

Et siste forhold kan være at et unødig høyt antall personell må sikkerhetsklareres på et for høyt nivå i forhold til det som er nødvendig. Dette fører igjen til unødig ressursbruk i klareringsprosessen, og også mulige unødvendige belastninger for enkeltindivider.

### 3.7.2 Undergradering eller underklassifisering

Et faremoment ved undergradering vil eksempelvis være at man unnlater å ta stilling til at mange ugraderte eller lavt graderte enkeltdeler til sammen vil kunne få et høyere graderingsnivå enn hver enkelt bestanddel. Sammenstilling av informasjon i store databaser er et område hvor nettopp denne type vurdering bør gjøres. Det er viktig å tenke gjennom detaljnivå i informasjonen, med

[21] sikkerhetslovens § 11

tanke på om den kan avsløre sårbarheter, at man kan koble sammen informasjon på en måte som avslører kapasiteter, sårbarheter og gjensidige avhengigheter på en måte man opprinnelig ikke hadde tenkt seg.

Erfaringsmessig forekommer det at informasjon ikke graderes eller undergraderes for å unngå å måtte følge et sikkerhetsregime som oppfattes som byrdefullt. Dette eksempelvis for å muliggjøre forsendelse av informasjon over Internett eller behandling av informasjon i et ønsket informasjonssystem. I en verdivurdering er ikke dette relevante momenter å ta i betraktning. Unnlatelse av å gradere eller en undergradering ut fra slike betraktninger vil være å anse som et sikkerhetsbrudd.

## 3.8 Sammenstilling av informasjon

En vurdering vil være om sammenstilling av ugradert og åpen informasjon utgjør en så verdifull kunnskapsbase at den er skjermingsverdig i henhold til sikkerhetsloven fordi den samlet og sammenstilt berører rikets sikkerhet eller vitale nasjonale sikkerhetsinteresser. Det kan eksempelvis være sammenstilling av data i store databaser hvor de enkelte delene/kildene hver for seg er ugraderte.

Spesielt viktig er det å foreta en verdivurdering når informasjonen har en stor detaljeringsgrad og kommer inn under kategorien risiko- og sårbarhetsinformasjon[22].

Ved sammenstilling av informasjon fra forskjellige graderingsnivåer er hovedregelen at det er den høyeste graderingen som er førende på den samlede graderingen (se også pkt 3.9 om punktgradering). Men den samlede informasjonsmengden bør være gjenstand for en verdivurdering med tanke på om de enkelte informasjonsbitene til sammen faktisk representerer en høyere verdi. Utfallet av en verdivurdering kan være at hvert enkelt informasjonselement beholder sin gradering, men at lagringsmediet for den samlede informasjonen gis den høyeste graderingen.

Sammenstilt sikkerhetsgradert informasjon som inneholder komponenter fra ulike utenlandske myndigheter og/eller internasjonale organisasjoner skal ikke nedgraderes eller avgraderes uten skriftlig forhåndssamtykke fra kompetent myndighet i det aktuelle land eller organisasjon. Ved gjenbruk og sammenstilling av slik type informasjon må det klart kunne identifiseres hvem som er informasjonseier av de enkelte delene. Dette kan gjøres gjennom punktgradering som også viser eierskap. Selve dokumentet bør i tillegg påføres norsk gradering.

I denne forbindelse kan nevnes den såkalte ”Liste-saken” som ble behandlet i rettsapparatet på 1980-tallet, hvor spørsmål om ytringsfrihet og rikets sikkerhet i fredstid ble aktualisert. Det dreide seg om en enkeltperson, som, nærmest som et ledd i privat etterretningsvirksomhet, samlet inn åpent tilgjengelig materiale om ansatte i overvåkings-, etterretnings- og sikkerhetstjenesten. Lister ble utarbeidet og overlatt til to journalister, som siden ble dømt for å ha tatt imot materialet.

## 3.9 Punktgradering

Å punktgradere informasjon vil si at en verdivurderer avsnitt for avsnitt i et dokument og fastsetter gradering på hvert avsnitt. Det fullstendige dokumentet skal graderes med den høyeste sikkerhetsgrad som er benyttet i dokumentet. Informasjonseiere oppfordres til å punktgradere sikkerhetsgradert informasjon ut fra flere hensyn. Det blir enklere å distribuere et dokument til en større brukergruppe hvis en f eks kan utelate de høyest graderte avsnittene eller samle dem i et vedlegg til slutt som ikke nødvendigvis tilflyter alle mottakere av hoveddokumentet. Et annet moment er at det blir lettere for mottagere av sikkerhetsgradert informasjon å gjenbruke deler av den i sine dokumenter. Det understrekes at det kun er informasjonseier som kan nedgradere sikkerhetsgradert informasjon, og derfor må det tydeliggjøres hvor sikkerhetsgradert informasjon er hentet fra.

Ved sammenstilling av informasjon fra mange kilder er det viktig å identifisere hvem som er informasjonseier til de enkelte delene. Se også pkt 3.8 om sammenstilling av utenlandsk sikkerhetsgradert informasjon. Mer om hvordan man punktgraderer og praktisk merker dokumenter finnes i forskrift om informasjonssikkerhet kapittel 2A og 4A.

[22] Se oversikt i vedlegg A.3 over virkeområdene til sikkerhetsloven, offentleglova og Beskyttelsesinstruksen

## 3.10 Ned- og avgradering

Sikkerhetsloven påpeker at det ikke skal nyttes mer inngripende midler og metoder enn det som fremstår som nødvendig i forhold til den aktuelle sikkerhetsrisiko og omstendighetene for øvrig.[23] Dette innebærer at gradering ikke skal skje i større utstrekning enn nødvendig, og at det ikke skal brukes høyere sikkerhetsgrad enn nødvendig.[24] Dette er viktig for å unngå å belaste administrative og økonomiske systemer mer enn strengt tatt påkrevd.

Sikkerhetsgradert informasjon bør derfor være gjenstand for vurdering når rammefaktorene for selve graderingen endres. Dette kan være informasjon som er av stor betydning å beskytte for en spesiell tidsperiode, f.eks. en forhandlingsposisjon, som etter at hendelsen har funnet sted ikke lenger er kritisk.

Et spørsmål man må stille seg er hvor lenge graderingen av den aktuelle informasjonen skal opprettholdes. Normalt skal tidsangivelsene 2 eller 5 år benyttes, og i prinsippet skal graderingen bortfalle senest etter 30 år. Andre tidsangivelser, herunder inntreden av bestemt begivenhet, kan benyttes dersom det er mer praktisk.

Det er viktig å merke seg at virksomhet som foretar omgradering skal underrette alle som har mottatt informasjonen om endringen.

Om nedgradering og omgradering, se nærmere i sikkerhetslovens § 11, samt forskrift om informasjonssikkerhet kapittel 2B, C og D.

## 3.11 Informasjon på Internett

Informasjon som ligger tilgjengelig på Internett er åpen informasjon. Det skal derfor ikke forekomme at sikkerhetsgradert informasjon publiseres på Internett, da det vil være et sikkerhetsbrudd. I tillegg er det å benytte Internett som informasjonskanal forbudt for sikkerhetsgradert informasjon. Generelt kan man si at tilgang til informasjon om et samfunns sårbare punkter kan være med på å øke kapasiteten hos ondsinnede aktører til å gjennomføre anslag. Man må også være oppmerksom på, og vurdere informasjon som legges ut i lys av, at den kan sammenstilles med annen tilgjengelig (sårbarhets)informasjon. NSM understreker derfor at det er viktig å tenke gjennom og skape bevissthet rundt hva virksomheten legger ut på Internett av informasjon som kan karakteriseres som risiko- og sårbarhetsinformasjon[25]. Slik informasjon, f eks om detaljer i beredskapsplaner eller tegninger og kart over kritisk infrastruktur, kan ha en høy nytteverdi for en utenforstående trusselaktør. Det vises til en oversikt i vedlegg A.2 over type informasjon det kan være viktig å verdivurdere også i forhold til hvorvidt det skal publiseres på Internett.

## 3.12 Skadereduserende tiltak for å oppnå redusert klassifisering

Siden skadepotensialet er en så viktig komponent i forhold til å fastsette verdien (og dermed sikkerhetsklassifiseringen), er det klart at en reduksjon av dette vil kunne ha en gunstig virkning. Det er ikke noe mål i seg selv å fastsette høyest mulig gradering på informasjon eller objekter. Det er også et lovfestet prinsipp at sikkerhetsgradering ikke skal skje i større utstrekning enn nødvendig, eller med høyere sikkerhetsgrad enn nødvendig. Tiltakene som kan være nødvendig for å beskytte for eksempel skjermingsverdige objekter kan i noen tilfeller vise seg å bli omfattende, kostbare og skape praktiske problemer til daglig.

Dersom det etter en verdivurdering (og en mer omfattende risikovurdering) viser seg at et objekt representerer en kritisk verdi for samfunnet, bør det vurderes om det kan gjøres tiltak for å redusere denne faktoren. Eksempelvis kan det etableres løsninger hvor funksjonene som ivaretas ved ett objekt også kan ivaretas et annet sted.

---

[23] Sikkerhetsloven § 6

[24] Sikkerhetsloven § 11 og forskrift om informasjonssikkerhet kap 2.

[25] NSM har utarbeidet et eget hefte kalt ”Internett og informasjonssikkerhet” som tar for seg denne problematikken. Det er bla utarbeidet en liste med 10 anbefalinger om hva en virksomhet bør tenke på i forbindelse med publisering av informasjon på Internett.

Lavere sikkerhetsgradering av informasjon kan for eksempel oppnås ved at de deler av informasjonen som medfører høyere verdifastsettelse tilsløres eller anonymiseres. Dette kan være nødvendig dersom det er behov for å gjøre tilgjengelig hovedinnholdet i en informasjonsmengde, men dette vanskeliggjøres ved at mulighetene for å beskytte denne ikke finnes i tilstrekkelig grad. Selvfølgelig må den informasjonen som var utgangspunktet for dette tiltaket beskyttes i henhold til den verdi og sikkerhetsgradering som gjelder for den.

## 3.13 Tjenstlig behov og autorisasjon

Det er et grunnleggende prinsipp at sikkerhetsgradert informasjon kun skal gjøres tilgjengelig for de som har et tjenstlig behov. Dette for å motvirke utilsiktet spredning. Prinsippet om tjenstlig behov er nedfelt i sikkerhetsloven § 12.[26] Et tjenstlig behov vil være utledet ut fra den funksjon vedkommende er satt til å utøve, dvs. hvilke oppgaver som skal utføres og hvorvidt tilgang til sikkerhetsgradert informasjon er nødvendig for å utføre oppgaven. Vedkommende må i tillegg inneha det riktige sikkerhetsklareringsnivå[27] tilsvarende den gradering informasjonen har, samt ha vært gjennom en autorisasjonsprosess av virksomhetens leder eller den som en har bemyndiget.[28] En har ikke automatisk tilgang til all type informasjon som er merket med den sikkerhetsgradering som samsvarer med sikkerhetsklareringen.

Prinsippet om tjenstlig behov tilsvarer det engelske ”need-to-know”. Man kan si at prinsippet har til hensikt å ikke spre informasjon unødig, da man i størst mulig grad ønsker å beholde kontrollen med hvem som får innsikt i informasjonen. Det påhviler et ansvar for informasjonsutstedere og informasjonsforvaltere å distribuere skjermingsverdig informasjonen til de riktige funksjoner/miljøer.

I denne sammenheng kan det være på sin plass å påpeke behovet for kunnskapsdeling (need-to-share). Hensikten med kunnskapsdeling er at flest mulig med tilsvarende sikkerhetsklareringsnivå skal kunne få tilgang på relevant sikkerhetsgradert informasjon. Det er derfor viktig at prinsippet om tjenstlig behov ikke benyttes av andre årsaker enn de rent sikkerhetsmessige.

Spredning av sikkerhetsgradert informasjon ut over hva som kan begrunnes ut fra det rent tjenstlige behov er ikke mulig innenfor rammen av gjeldende lovverk.

## 3.14 Økonomiske og administrative konsekvenser av verdivurdering

I fastsettelse av nivå på sikkerhetsgradering iht. sikkerhetsloven bør det understrekes at økonomiske og administrative konsekvenser ikke skal influere på avgjørelsen. En verdivurdering skal kun fokusere på hvorvidt, og i hvilken grad, informasjonen eller objektet omfattes av begrepene *rikets selvstendighet og sikkerhet* eller andre *vitale nasjonale sikkerhetsinteresser*. Økonomiske og administrative konsekvenser av en beslutning om gradering/klassifisering kan etter sikkerhetslovens § 11 ikke lovlig vektlegges i verdivurderingen.

[26] Sikkerhetsloven § 12, *Plikt til å beskytte sikkerhetsgradert informasjon*

[27] Sikkerhetsklarering: Avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad, se sikkerhetsloven § 3 pkt 16

[28] En autorisasjon er en avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad, se sikkerhetsloven § 3 pkt. 17.

# 4 Sikkerhetsloven og forhold til annet regelverk

Prinsippet om offentlighet er fastsatt i offentleglovas § 3[29]. Hovedregelen er at forvaltningens saksdokumenter er offentlige så langt det ikke er gjort unntak i loven.

Det finnes regelverk utover sikkerhetsloven som er utformet med tanke på skjerming av opplysninger og objekter. De viktigste blir redegjort for nedenfor. I de tilfeller hvor opplysningenes art ligger i et grenseland, det vil si at hensikten med skjerming kan vurderes forskjellig opp mot de enkelte lovers og reglers intensjon, vil det være en skjønnsmessig vurdering som blir avgjørende for verdivurderingen.

## 4.1 Offentleglova

Offentleglovas formål er "å leggje til rette for at offentleg verksemd er open og gjennomsiktig, for slik å styrkje informasjons- og ytringsfridommen, den demokratiske deltakinga, rettstryggleiken for den enkelte, tilliten til det offentlege og kontroll frå ålmenta".

Offentleglova gir ikke anvisning på hvordan et dokument som er unntatt offentlighet skal behandles og oppbevares for å hindre innsyn i dokumentet. Offentleglova gir hjemmel for å hindre innsyn, men gir ikke informasjonen i seg selv beskyttelse slik sikkerhetsloven gjør.

Lovens § 13 definerer nærmere at opplysninger undergitt lovbestemt taushetsplikt skal unntas offentlighet. Lovens kapittel 3 gir ulike unntak for innsynsretten, særlig kan nevnes § 20 som gir unntak av hensyn til Norges utenrikspolitiske interesser, § 21 som omhandler unntak av hensyn til nasjonale forsvars- og sikkerhetsinteresser og § 23 om unntak av hensyn til det offentliges forhandlingsposisjon m.m.

## 4.2 Beskyttelsesinstruksen

Beskyttelsesinstruksen[30] kommer til anvendelse når dokumenter trenger spesiell beskyttelse og det ikke inneholder opplysninger som faller inn under sikkerhetsloven. Beskyttelsesinstruksen gir bestemmelser om beskyttelse av informasjon og gjelder for statsforvaltningen.

For å kunne beskytte opplysninger etter denne instruksen må opplysningene kunna unntas offentlighet etter offentleglovas unntaksbestemmelser. Beskyttelsesinstruksens § 3 lyder: "Gradering av et dokument skal bare foretas når det kan unntas offentlighet i medhold av offentleglova og skadevirkninger som nevnt i § 4 kan inntreffe":

- STRENGT FORTROLIG nyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.

- FORTROLIG nyttes dersom det vil kunne skade offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.

Informasjon gradert etter Beskyttelsesinstruksen skal skje etter bestemmelsene som gjelder for informasjon som er sikkerhetsgradert BEGRENSET. Se for øvrig den skjematisk oversikt over sikkerhetsloven, offentleglova og Beskyttelsesinstruksens vedlegg A 3.

[29] Lov om rett til innsyn i dokument i offentleg verksemd av 19. mai 2006 nr. 16

[30] Forskrift av 17. mars 1972 nr 3352 (senest med endringer ved forskrift av 23. januar 2009 nr 50) Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn det som er nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen)

## 4.3 Personopplysningsloven

I personopplysningslovens § 13[31] stilles også krav til beskyttelse av informasjon. Etter forskrift om behandling av personopplysninger kapittel 2 finnes funksjonelle krav til informasjonssikkerhet. Til hjelp i arbeidet med å anslå taps- eller skadepotensial er det aktuelt å avdekke om personopplysningene er *sensitive*, se lovens § 2. Dette begrepet skal ikke oppfattes som en sikkerhetsgradering i seg selv. Personopplysningsloven benytter begrepet for vidt forskjellige opplysninger, også for slike som i seg selv ikke utløser særlige krav til sikkerhetstiltak (eks. medlemskap i fagforeninger). Det sier imidlertid noe om forventet diskresjon, det vil si angir behov for konfidensialitet – men det må understrekes at begrepet ikke sier noe om andre behov (tilgjengelighet eller integritet).

## 4.4 Sektorvise regelverk/lover

Innen ulike sektorer i samfunnet finnes regel- og planverk som i varierende grad også omfatter behov for skjerming av informasjon og objekter. Den enkelte virksomhet er forpliktet til å sette seg inn i de angjeldende regelverk.

### 4.4.1 Anskaffelser

Lov om offentlige anskaffelser[32] (LOA), og forskrifter gitt med hjemmel i denne regulerer anskaffelsesvirksomheten for staten. Lovens § 3 og anskaffelsesforskriftens § 1-3 hjemler i visse tilfeller unntak fra det alminnelige anskaffelsesregelverket ved anskaffelser som krever særskilte sikkerhetstiltak, f. eks fordi anskaffelsen involverer sikkerhetsgradert informasjon. Om unntakene kommer til anvendelse må imidlertid bero på en konkret vurdering i det enkelte tilfelle.

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

[32] Lov om offentlige anskaffelser av 16. juli 1999 nr. 69

# Vedlegg

## A.1 Liste over begreper og terminologi

## A.2 Eksempler på informasjon og objekter som kan være gjenstand for verdivurdering

## A.3 Skjematisk oversikt over sikkerhetslovens, offentleglovas og Beskyttelsesinstruksens virkeområde

## A.1 LISTE OVER BEGREPER OG TERMINOLOGI

| | |
|---|---|
| Anskaffelsesmyndighet | Et forvaltningsorgan som har til hensikt å anskaffe, eller har anskaffet, varer, tjenester fra rettssubjekt som ikke er et forvaltningsorgan |
| Autorisasjon | Avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad.(sikkerhetsloven § 3 pkt. 17) |
| Dokument | En logisk avgrenset informasjonsmengde som er lagret på et medium for senere lesing, lytting, fremføring eller overføring (forskrift om informasjonssikkerhet § 1-2 nr 1) |
| Forebyggende sikkerhetstjeneste | Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet |
| Informasjon | Enhver form for opplysninger i materiell eller immateriell form (sikkerhetsloven § 3 pkt. 7) |
| Intensjon | Personers eller organisasjoners vilje og motivasjon til å realisere en trussel |
| Kapasitet | De ressurser og den kompetanse som er nødvendig for å realisere en trussel. |
| Kompromittering | Tap eller mistanke om tap av konfidensialitet, integritet eller tilgjengelighet for skjermingsverdig informasjon, herunder uønsket avhending, modifisering eller ødeleggelse. (forskrift om sikkerhetsadministrasjon § 1-2 pkt. 3) |
| Risiko | Uttrykk for den fare som uønskede hendelser representerer for informasjon/objekter av skjermingsverdig karakter. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene. |
| 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 pkt. 4) |
| Sikkerhetsadministrasjon | Internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetenes aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt i og i medhold av sikkerhetsloven. (forskrift om sikkerhetsadministrasjon § 1-2 pkt. 1) |
| Sikkerhetsbrudd | Brudd på bestemmelse om sikkerhetstiltak gitt i sikkerhetsloven eller forskrifter til sikkerhetsloven. (forskrift om sikkerhetsadministrasjon § 1-2 pkt. 4) |
| Sikkerhetsgradert anskaffelse | Anskaffelse, foretatt av anskaffelsesmyndighet, som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker. |

| | |
|---|---|
| | (sikkerhetsloven § 3 pkt. 14) |
| Sikkerhetsgradert informasjon | Informasjon som er merket med sikkerhetsgrad i henhold til reglene i sikkerhetsloven § 11 |
| Sikkerhetsklarering | Avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad. (sikkerhetsloven § 3 pkt. 16) |
| Sikkerhetstruende hendelse | Sikkerhetstruende virksomhet, kompromittering av skjermingsverdig informasjon og grove sikkerhetsbrudd.<br><br>(forskrift om sikkerhetsadministrasjon § 1-2) |
| Sikkerhetstruende virksomhet | Forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandliner, samt medvirkning til slik virksomhet. (sikkerhetsloven § 3 pkt. 2) |
| Skjermingsverdig informasjon | Informasjon som skal merkes med sikkerhetsgrad i henhold til sikkerhetslovens § 11. Det skilles mellom sikkerhetsgradene STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT og BEGRENSET. Vurderingen av hvilken sikkerhetsgradering informasjonen skal få, er basert på en vurdering av hvilken skade på rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser som ville oppstå, dersom informasjonen ble kompromittert. (sikkerhetsloven § 3 pkt. 8) |
| Skjermingsverdig objekt | Eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale, nasjonale sikkerhetsinteresser. (sikkerhetsloven § 3 pkt. 12) |
| Spionasje | Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt. (sikkerhetsloven § 3 pkt. 3) |
| Terrorhandlinger | 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 pkt. 5) |
| Trussel | Ethvert forhold eller enhver enhet med potensial til å forårsake en uønsket, negativ hendelse. |
| Trusselaktør | En person, organisasjon eller et objekt som ønsker og er i stand til/evner å utløse en uønsket, negativ hendelse. ”Ønsket” kan relateres til intensjon, ”evne” kan relateres til kapasitet. |
| Verdivurdering | En analyse som har til hensikt å identifisere hvilke objekter og hvilken type informasjon som er så viktig av hensyn til rikets sikkerhet og vitale nasjonale sikkerhetsinteresser at de må skjermes. |
| Virksomhet | Et forvaltningsorgan eller annet rettssubjekt som sikkerhetsloven gjelder for, jf sikkerhetsloven § 2. |

## A.2 EKSEMPLER PÅ TYPE INFORMASJON OG OBJEKTER SOM KAN VÆRE GJENSTAND FOR VERDIVURDERING:

- Beredskapsplanverk
- Detaljinformasjon om medarbeidere i operative avdelinger
- Detaljert informasjon om lagre for strategiske ressurser
- Detaljinformasjon om samfunnskritiske forsknings- og utviklingsprosjekter
- Etterretningsrapporter
- Informasjon som i vesentlig grad kan vanskeliggjøre opprettholdelse av norsk økonomisk evne
- Metode, mål og kapasiteter til etterretnings-, overvåknings- og sikkerhetstjenestene
- Operative planer
- Oversikt over iverksatte forebyggende sikkerhetstiltak
- Oversikt over fysiske sikringstiltak iht. sikkerhetsloven
- Oversikt over sårbarheter som kan utnyttes av utenforstående
- Oversikt over sårbarheter ifm beskyttelse av farlig biologisk, kjemisk og radiologisk materiale
- Oversikt over sårbarheter ifm transportknutepunkter/flyplassikkerhet
- Plantegninger over samfunnskritiske bygninger
- Politiske forhandlingsstandpunkter overfor motparter/andre land
- Planverk
- Reisevirksomhet til kritisk personell
- Risiko- og sårbarhetsinformasjon
- Samfunnskritiske funksjoner
- Sensitive stillinger/funksjoner
- Sikkerhetsorganisasjon
- Sikkerhetssystemer rundt virksomhetskritisk IKT
- Store sentraliserte databaser
- Virksomhetskritiske informasjonssystemer
- Virksomhetskritisk nasjonal infrastruktur

## A.3 SKJEMATISK OVERSIKT OVER SIKKERHETSLOVENS, OFFENTLEGLOVAS OG BESKYTTELSESINSTRUKSENS VIRKEOMRÅDE

| Lov- og regelverk[33] | Statlig sektor | Kommunal sektor | Privat sektor |
|---|---|---|---|
| **Sikkerhetsloven:**<br><br>Gir hjemmel for beskyttelse av informasjon som kan true rikets selvstendighet og sikkerhet og andre vitale nasjonale interesser om den ble kjent for uvedkommende.<br><br>Angir hvordan dokumenter skal behandles for å hindre innsyn fra uvedkommende gjennom etablering av et helhetlig beskyttelsesregime. Kun utsteder kan endre sikkerhetsgradering. | Dekker risiko- og sårbarhets-informasjon i forhold til rikets sikkerhet, informasjon om samfunnskritisk virksomhet og funksjoner av nasjonal betydning | Det samme som for statlig sektor | Dekker det samme som for statlig sektor under forutsetning at:<br><br>1. Virksomheten er en leverandør i forbindelse med en sikkerhetsgradert anskaffelse, eller<br><br>2. Det er fattet vedtak om at loven skal gjelde for den aktuelle private virksomhet. |
| **Offentleglova:**<br><br>Krever at opplysninger undergitt lovbestemt taushetsplikt er unntatt fra innsyn.<br><br>Gir hjemmel for å unnta fra offentlighet informasjon som omhandler Norges utenrikspolitiske interesser, hensyn til nasjonale forsvars- og sikkerhetsinteresser og det offentliges forhandlingsposisjon<br><br>Angir ikke retningslinjer om dokumentbehandling og beskyttelse av informasjonen.<br><br>Forplikter ikke mottaker av dokument til å holde dokumentet unntatt offentlighet. | Dekker risiko- og sårbarhets-informasjon hvor innsyn kan lette gjennomføring av straffbare handlinger.<br><br>Hindrer innsyn, men gir ikke informasjonen beskyttelse | Det samme som for statlig sektor | Omfattes ikke |
| **Beskyttelsesinstruksen:**<br><br>Gir hjemmel for beskyttelse av informasjon som om den ble kjent kan forårsake skade for offentlige interesser, en bedrift, institusjon eller enkeltperson.<br><br>Angir dokumentbehandling. | Dekker risiko- og sårbarhets-informasjon som ikke dekkes av Sikkerhetsloven.<br><br>Hindrer innsyn og gir beskyttelse som for BEGRENSET | Omfattes ikke | Omfattes ikke |

[33] Ikke uttømmende – kun medtatt de bestemmelser som kan ha en direkte relevans opp mot beskyttelse av risiko- og sårbarhetsinformasjon