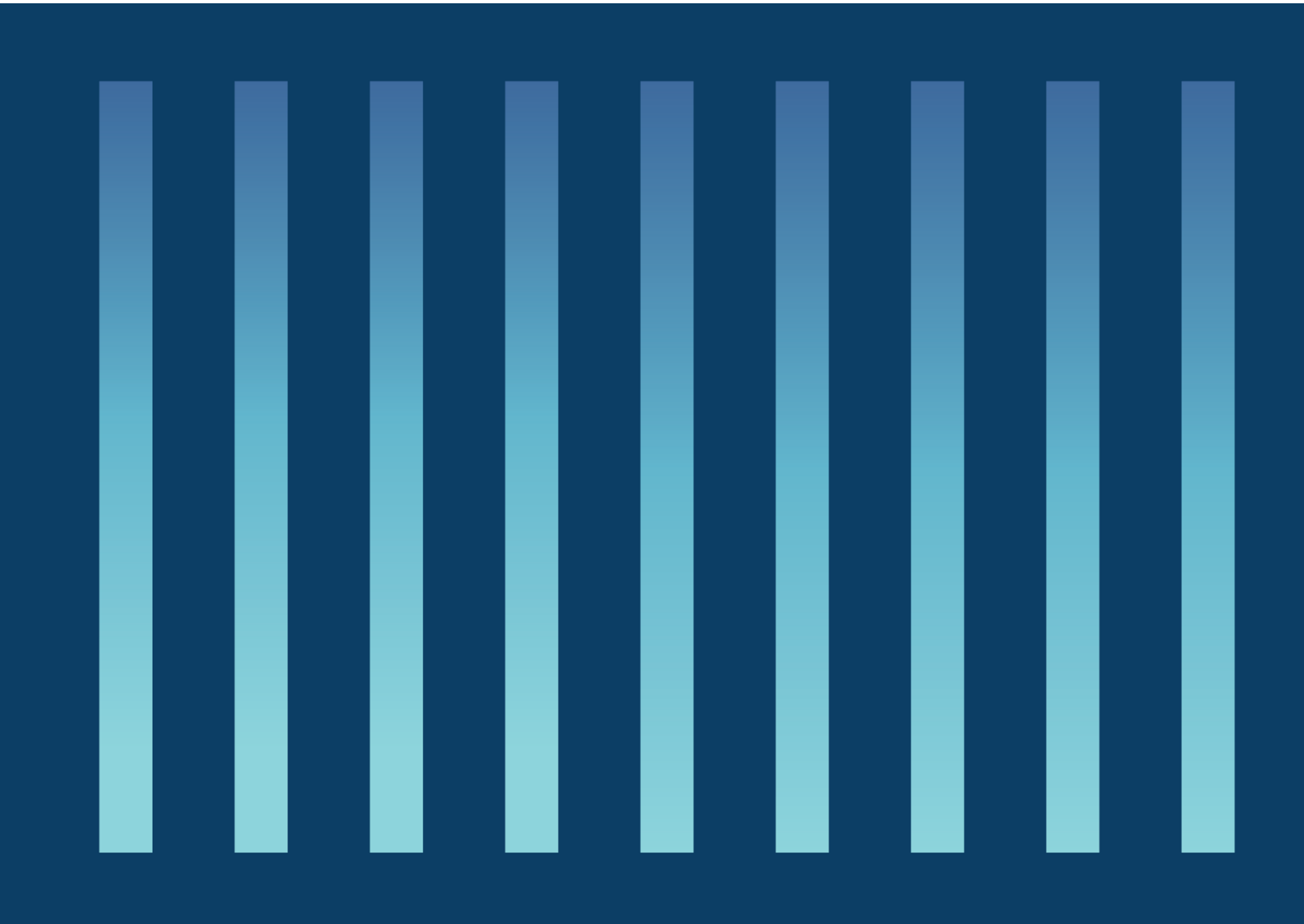
NASJONAL
SIKKERHETSMYNDIGHET

Håndbok i verdivurdering av informasjon

Fremgangsmåte for vurdering av beskyttelsesbehov for informasjon av hensyn til nasjonale sikkerhetsinteresser

Versjon: 1



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

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

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

NSMs håndbøker og tekniske råd gir utfyllende anbefalinger om hvordan regelverkets funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen. Disse må ses i sammenheng med NSMs veiledere til lov og forskrift.

NSM gir i tillegg ut veiledere som gir uttrykk for NSMs syn på hvordan lov og forskrift er å forstå.

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

INNHOLD

Tema for håndbok

Nasjonal sikkerhetsmyndighet har utgitt en veileder i verdivurdering av informasjon. Denne håndboken er ment å supplere veilederen ved at den beskriver en fremgangsmåte for verdivurdering av informasjon. Håndboken er avgrenset til å omfatte fremgangsmåte for vurdering av konfidensialitetsbehov, og omhandler ikke tilgjengelighet- og integritetbehov. Håndboken dekker derfor kun verdivurderinger som gjøres for å vurdere om informasjonen skal sikkerhetsgraderes. Fremgangsmåten dekker ikke vurderinger om informasjonen er skjermingsverdig ugradert. Formål

Formålet med denne håndboken er å hjelpe den som verdivurderer:

- vurdere hvorvidt uvedkommendes tilgang til informasjonen kan forventes å forårsake skade på nasjonale sikkerhetsinteresser, gjennom å
- identifisere og beskrive skadefølger, for å kunne
- konkludere om informasjon må beskyttes i henhold til kravene i sikkerhetsloven av hensyn til nasjonale sikkerhetsinteresser.

Gode verdivurderinger kan være avgjørende for ivaretakelsen av nasjonale sikkerhetsinteresser. En god verdivurdering forutsetter kunnskap om fremgangsmåten for verdivurdering av informasjon, temaet som informasjonen omhandler, og om begrepet nasjonale sikkerhetsinteresser. Å gi informasjon uriktig sikkerhetsgrad kan øke risiko for sikkerhetstruende virksomhet. Uriktig sikkerhetsgrad omtales ofte som en *feilgradering*.

Feilgraderinger hvor informasjonen gis for høy sikkerhetsgrad kalles for *overgradering*. Overgraderinger fører til at virksomheten må implementere mer omfattende barrierer enn det som i realiteten er nødvendig. Utstrakt overgradering av informasjon kan også føre til at graderingsnivået ikke respekteres av virksomhetens ansatte. Et siste forhold kan være at et unødig høyt antall personell må sikkerhetsklareres på et for høyt nivå sammenlignet med det egentlige behovet. Dette fører igjen til unødig ressursbruk i klareringsprosessen, og også mulige unødvendige belastninger for enkeltindivider.

Feilgraderinger hvor informasjonen gis for lav sikkerhetsgrad kalles for *undergradering*. Ettersom sikkerhetsgraden er førende for hvilke barrierer som implementeres for å beskytte informasjonens konfidensialitet, kan undergradering av informasjon resultere i at virksomheten ikke beskytter informasjonen tilstrekkelig, sett i lys av skadepotensialet informasjonen representerer. Erfaringsmessig forekommer det at informasjon ikke gis en sikkerhetsgrad, eller gis en lavere sikkerhetsgrad, for å unngå å måtte implementere flere eller mer omfattende sikkerhetstiltak. Dette kan eksempelvis være for å muliggjøre forsendelse av informasjon over internett eller behandling av informasjon i et ønsket informasjonssystem. Bekvemmelighetshensyn er ikke relevante momenter å ta i betraktning når beskyttelsesbehov av hensyn til nasjonale sikkerhetsinteresser skal vurderes. Unnlatelse av å gradere eller en undergradering ut fra slike hensyn vil være å anse som et sikkerhetsbrudd.

1. Virksomhetens rolle

Det er virksomheten som tilvirker informasjonen som skal sikkerhetsgradere og merke informasjonen dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende, jf. SL §5-3, 1. ledd. Begrepet nasjonale sikkerhetsinteresser er definert i § 1-5 nr. 1. Virksomheten er dermed pliktig å gjennomføre en verdivurdering som grunnlag for en eventuell sikkerhetsgradering av informasjonen.

Informasjon skal fortrinnsvis være gjenstand for løpende verdivurdering under tilvirkingsprosessen, altså underveis i produksjonen av informasjonen. Det vil imidlertid i noen tilfeller være behov for å sikkerhetsgradere tidligere tilvirket informasjon som ikke tidligere har vært håndtert i henhold til kravene i sikkerhetsloven. Dette kan eksempelvis være tilfellet for virksomheter som blir omfattet av sikkerhetsloven ved vedtak etter SL § 1-3, som følge av et departements vurdering av at virksomheten er av avgjørende betydning for grunnleggende nasjonale funksjoner. Dette temaet omhandles under spørsmålet «*kan informasjonen kontrolleres?*» i del 1 av fremgangsmåten for verdivurdering.

Virksomheten står fritt til å implementere egne prosesser og retningslinjer for verdivurdering og beslutninger om sikkerhetsgradering. I noen virksomheter kan det være hensiktsmessig å etablere egne funksjoner for å bistå i verdivurderingsprosessen. Håndbokens siste del omhandler bruk av virksomhetsinterne retningslinjer for verdivurdering.

2. Fremgangsmåte

Fremgangsmåten for å vurdere hvorvidt informasjon har et beskyttelsesbehov av hensyn til nasjonale sikkerhetsinteresser består av en rekke spørsmål som hjelper den som verdivurderer til å fatte en beslutning om sikkerhetsgradering. Gjennom besvarelsen av disse spørsmålene bygger den som verdivurderer argumentasjon for hvorfor informasjon skal, eller ikke skal, sikkerhetsgraderes, og eventuelt på hvilket nivå. Fremgangsmåten innebærer både å vurdere *opplysninger* hver for seg, og som samlede informasjonsmengder, eksempelvis i et dokument[1]. Begrepet *opplysninger* brukes altså her som en delmengde av en større informasjonsmengde. I tilfeller hvor en avgrenset informasjonsmengde fremkommer i et dokument, så vil en opplysning som regel regnes som enkeltsetninger eller ord.

Del 1. Før verdivurderingen

Den som skal verdivurdere informasjon må ha god kunnskap om temaet som informasjonen omhandler. For å ha tilstrekkelig grunnlag til å vurdere potensielle skadefølger ved tap av konfidensialitet bør annen faglig eller teknisk ekspertise konsulteres ved behov. Man bør også danne seg et bilde av hvilken annen informasjon som er tilvirket om temaet, og hvorvidt det er andre

[1] *dokument:* en logisk avgrenset mengde med informasjon som er lagret på et medium for senere lesing, lytting, framføring, overføring eller lignende (§ 2 b, forskrift om virksomheters arbeid med forebyggende sikkerhet)

opplysninger om temaet som tidligere er blitt publisert eller på annen måte er allment kjent. I denne forberedende fasen er det tre spørsmål den som skal verdivurdere må ta stilling til.

Spørsmål 1: Er opplysningen, eller tilsvarende opplysninger, verdivurdert tidligere?

I noen tilfeller er det tidligere gjort vurderinger om hvorvidt opplysninger har et beskyttelsesbehov. Allerede sikkerhetsgraderte opplysninger kan ikke omgraderes av andre enn det regelverket åpner for, jf virksomhetssikkerhetsforskriften § 31 . Det kan også være at det tidligere er gjort vurderinger om hvorvidt tilsvarende informasjon skal sikkerhetsgraderes, tilsvarende dokumenter osv. I noen tilfeller er det snakk om en kombinasjon av «ny» (ikke tidligere verdivurdert) og «gammel» (tidligere verdivurdert) informasjon. Hvis en informasjonsmengde utelukkende består av tidligere verdivurderte opplysninger, så kan den som verdivurderer gå videre til spørsmålet om sammenstilling i selve verdivurderingsprosessen (Del 2., spørsmål 4).

Spørsmål 2: Kan informasjonen kontrolleres?

Virksomheten må ha tillit til at konfidensialiteten til informasjon som sikkerhetsgraderes er ivaretatt, og at den kan ivaretas. Virksomheten må derfor undersøke hvorvidt opplysningene tidligere er blitt publisert, eller på annen måte er eller har vært tilgjengelig for uvedkommende.

I noen tilfeller vil det være behov for å sikkerhetsgradere tidligere tilvirkede opplysninger som ikke tidligere har vært håndtert i henhold til kravene i sikkerhetsloven. Virksomheten må vurdere om beskyttelsestiltakene for sikkerhetsgradert informasjon har en faktisk sikkerhetsmessig merverdi, eller om opplysningene må anses som kompromitterte. Her vil det være naturlig å skille mellom åpent tilgjengelig informasjon, og informasjon som ikke har vært åpent tilgjengelig, og som har vært gjenstand for kontrollmekanismer.

Opplysninger som har (eller sannsynligvis har) vært eksponert for uvedkommende må håndteres som en sårbarhet. Det er ingen automatikk i at eksponerte opplysningen ikke lengre har et skadepotensiale og må avgraderes.

Spørsmål 3: Hvem er det informasjonen omhandler?

En virksomhet kan tilvirke informasjon som omhandler forhold ved andre virksomheter, uten at den andre virksomheten har verdivurdert denne informasjonen. Slike situasjoner kan oppstå i gjennomføringen av forskningsprosjekter, undersøkelser eller sammenstilling av informasjon fra ulike kilder. Ettersom skadefølgene ved tap av konfidensialitet omfatter en annen virksomhet, bør virksomheten som tilvirker informasjonen vurdere å konsultere den andre virksomheten i løpet av verdivurderingsprosessen, eller på annen måte be om virksomhetens vurdering av opplysningene.

Del 2. Verdivurderingsprosessen

Spørsmål 1: Omhandler opplysningen et forhold av betydning for nasjonale sikkerhetsinteresser?

Den som verdivurderer starter vurderingen med å ta stilling til hvorvidt opplysningen omhandler et forhold som er relatert til eller er av betydning for nasjonale sikkerhetsinteresser. Det at informasjonen kan relateres til forhold av betydning for nasjonale sikkerhetsinteresser, er en forutsetning for å sikkerhetsgradere informasjon. Disse interessene er definert i SL § 1-5, som

- landets suverenitet,
- territorielle integritet og
- demokratiske styreform,

og overordnede sikkerhetspolitiske interesser knyttet til

- øverste statsorganers virksomhet, sikkerhet og handlefrihet,
- forsvar, sikkerhet og beredskap,
- forholdet til andre stater og internasjonale organisasjoner,
- økonomisk stabilitet og handlefrihet, og
- samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.

Forhold av betydning for nasjonale sikkerhetsinteresser kan eksempelvis være Norges strategiske interesser i nordområdene, systemer for kommunikasjon mellom totalforsvarsaktører, og sikkerheten i valgprosesser og beskyttelse mot valgpåvirkning.

Den som verdivurderer må deretter danne seg et bilde av i hvilken grad gjeldende opplysninger er av betydning for nasjonale sikkerhetsinteresser. Formålet er å danne grunnlag for å vurdere skadepotensialet senere i prosessen. Et eksempel på argumentasjonsrekkefølge kan være

«*Kommunikasjon mellom totalforsvarsaktørene er avgjørende for totalforsvarets funksjonsevne, og totalforsvaret er sentralt i ivaretakelsen av nasjonale sikkerhetsinteresser. Dermed vil systemer for kommunikasjon mellom aktørene være et forhold av stor betydning for de nasjonale sikkerhetsinteressene*».

I noen tilfeller kan andre vurderinger knyttet til identifiserte grunnleggende nasjonale funksjoner (GNF), virksomheter av betydning for GNF, osv. være til hjelp i vurderingen av i hvilken grad gjeldende opplysninger er av betydning for nasjonale sikkerhetsinteresser.

Mer informasjon om nasjonale sikkerhetsinteresser og grunnleggende nasjonale funksjoner er beskrevet i NSMs veileder i departementenes identifisering av grunnleggende nasjonale funksjoner.

Spørsmål 2: Vurder kategoriene av informasjon som kan få skadefølger. Er opplysningen i en eller flere av disse?

Etter å ha slått fast at opplysningen omhandler forhold av betydning for nasjonale sikkerhetsinteresser, vil neste steg være å vurdere selve innholdet i opplysningen opp mot en rekke kategorier av

informasjon som kan ha et skadepotensiale[2]. Disse kategoriene har egenskaper som kan utnyttes til å forberede og gjennomføre sikkerhetstruende virksomhet, samt påvirke følgene av sikkerhetstruende virksomhet.[3] Opplysninger kan også anses å høre til flere kategorier i kombinasjon. Eksempelvis kan opplysninger anses å omhandle både kapasiteter og sårbarhetsvurderinger, eller utvikling og spesifikasjoner.

Skadevurderinger

Kategorien omfatter vurderinger av potensielle skadefølger ved sikkerhetstruende virksomhet om slik virksomhet skulle finne sted. Om slike skadevurderinger omhandler potensielt skjermingsverdige objekter eller infrastruktur etter SL § 7-1, pålegger VF § 57 virksomhetene å gradere vurderingene som BEGRENSET eller høyere. Tilsvarende skal opplysningen om klassifiseringsnivå og grunnlaget for klassifisering av skjermingsverdige objekter og infrastruktur være sikkerhetsgradert BEGRENSET eller høyere. En oversikt over samtlige eller et større antall klassifiserte objekter eller infrastrukturer skal sikkerhetsgraderes KONFIDENSIELT eller høyere. I vurderingen av hva som kan anses som «et større antall» bør virksomheten legge vekt på forholdet mellom objektene og infrastrukturene i oversikten. Er det snakk om en oversikt over alle skjermingsverdige objekter og infrastrukturer som understøtter én og samme GNF? En slik oversikt vil kunne ha et større skadepotensial enn en oversikt med objekter og infrastruktur som understøtter ulike GNF eller på annen måte ikke er i samme verdikjede.

Sårbarhetsvurderinger

Kategorien omfatter vurderinger av evne til å motstå sikkerhetstruende virksomhet eller å opprette ny stabil tilstand dersom en verdi er utsatt for sikkerhetstruende virksomhet. Opplysninger som inngår i en sårbarhetsvurdering kan omhandle svake ledd i motstandsevnen som gjør prosesser eller elementer sårbare for svikt. Det kan også omhandle hvor ofte svikt i motstandsevnen oppstår, og effekten ved svikt. Sentrale momenter i vurderingen av hvorvidt innholdet i sårbarhetsvurderinger har et skadepotensial er om opplysningene om svikt eller svake ledd kan utnyttes av en trusselaktør, og om disse opplysningene kan beskyttes mot utnyttelse.

Konsekvensvurderinger

Kategorien omfatter vurderinger av skadefølgene for nasjonale sikkerhetsinteresser dersom sikkerhetstruende virksomhet har inntruffet. Sentrale momenter i vurderingen av hvorvidt innholdet i konsekvensvurderinger har et skadepotensial vil være om opplysningene kan bekrefte for en motstander hvilken effekt og måloppnåelse sikkerhetstruende virksomhet har hatt.

Trusselvurderinger

Kategorien omfatter opplysninger som beskriver virksomhetens trusselbilde. Kategorien omfatter også vurderinger av trusselaktørers vilje til å utføre en handling, aktørens hensikt ved å utføre handlingen

[2] Skadevurderinger, sårbarhetsvurderinger, konsekvensvurderinger, trusselvurderinger, etterretning, sivilt- og militært beredskapsplanverk, opplysninger om spesifikasjoner, kapasiteter og kapabiliteter, opplysninger om kryptomateriell, opplysninger om Norges diplomati, opplysninger som omhandler vitenskap og teknologi, opplysninger om sikkerhetstiltak, opplysninger om hendelser i fortid (f.eks. rapporter om sikkerhetsbrudd eller gjennomførte øvelser), opplysninger om hendelser i fremtid (f.eks. scenarioer, besøk eller utvikling), opplysninger om militære og sivile operasjoner og EOS-tjenestenes kilder og metoder.

[3] Dette utelukker likevel ikke at informasjon som faller utenfor disse kategoriene likevel kan sikkerhetsgraderes, om den som verdivurderer kan beskrive et skadepotensial for nasjonale sikkerhetsinteresser.

(intensjon), samt vurderinger av trusselaktørers tilgjengelige ressurser, kunnskap og ferdighet, som forutsetninger for å utføre en handling (kapasitet).

Etterretning

Kategorien omfatter produkter av innsamling, evaluering, analyse, integrering og tolkning av tilgjengelig informasjon som omhandler andre aktørers intensjoner, kapasiteter og mål. Kategorien omfatter både produktet i seg selv, og hvordan produktet er produsert.

Sivilt- og militært beredskapsplanverk

Kategorien omfatter beskrivelser av sivil og militær samhandling, prosesser, tiltak og handlingsmåter i håndteringen av uønskede hendelser. Eksempelvis tiltak i Beredskapssystem for Forsvaret (BFF) og Sivilt Beredskapssystem (SBS), opplysninger om oppgavefordeling, beslutningsmyndighet, mobiliseringstider, og ordregang.

Opplysninger om spesifikasjoner, kapasiteter og kapabiliteter

Begrepet *spesifikasjon* omfatter en detaljert beskrivelse av design og materiale benyttet for å konstruere noe, men også forhold som omfatter operasjon og vedlikehold. Begrepet *kapabilitet* forstås som en kvalitet eller en type evne eller egenskap. For eksempel vil informasjon om våpen, sensorer, beslutningstagere, og sammenkoblingen av disse elementene, i kombinasjon med et konsept for hvordan elementene skal samvirke for å utføre oppgaver, være en kapabilitet. Begrepet *kapasitet* forstås som en kvantitativ egenskap som uttrykker volum eller størrelse[4]. Kategorien favner eksempelvis opplysninger om ytelsesgrenser, som fart, akselerasjon, høyde, vektbelastning, reaksjonstid, sensibilitet, rekkevidde, frekvens, varmebelastning, mv.

Opplysninger om kryptologi

Kategorien innbefatter alle forhold vedrørende kryptologi, inkludert utvikling, metoder, kapasiteter, og sårbarheter innen både kryptografi og kryptoanalyse. For kryptosystemer som skal brukes for å beskytte sikkerhetsgradert informasjon er det konkrete bestemmelser for sikkerhetsgradering av spesifikke typer informasjon. Bestemmelsen i kryptosikkerhetsforskriften § 26 sier at kryptoregnskap og beholdningsrapporter med oppgave over kryptonøkler skal graderes KONFIDENSIELT. NSM bestemmer for det enkelte tilfelle sikkerhetsgrad for informasjon om kryptonøklers gyldighetsperiode. Regnskap og rapporter sikkerhetsgraderes etter sitt innhold, likevel minst BEGRENSET. § 33 i samme forskrift sier at det ved tilintetgjøring av kryptomateriell skal utferdiges tilintetgjøringsrapport. Tilintetgjøringsrapporten skal inneholde et løpenummer, kryptomateriellets tittel, utgave, antall og registreringsnummer. Rapporter på papir skal være påført teksten «Siste post» etter siste linje. Etter tilintetgjøringen skal rapporten signeres av det personellet som har utført tilintetgjøringen og graderes KONFIDENSIELT.

Opplysninger om Norges diplomati

Kategorien omfatter opplysninger som omhandler Norges posisjoner og muligheter i forhandlinger med andre stater. Den omfatter også kommentarer og vurderinger om andre staters diplomatiske forbindelser, posisjoner og forhandlingsmuligheter.

[4] Forsvarets policy for konseptutvikling og eksperimentering (Concept Development and Expermenation CDE) 2004

Opplysninger som omhandler vitenskap og teknologi

Kategorien kan omfatte vitenskap og teknologi som kun Norge har, eller antas å ha, kjennskap til, har utviklet, eller på annen måte besitter. Sentrale vurderingskriterier er om opplysninger om kunnskap og teknologi, hvis de blir kjent, kan resultere i at andre nasjoner kan utvikle tilsvarende kapasiteter eller nå samme kunnskapsnivå. Videre, om slike opplysninger kan føre til at en fremmed stat øker sin innsats på feltet, med det formål å minske Norges forsprang.

Opplysninger om sikkerhetstiltak

Kategorien omfatter implementerte eller planlagte sikkerhetstiltak for å beskytte virksomhetens verdier mot sikkerhetstruende virksomhet, eksempelvis hvilke konsekvensreduserende tiltak som er implementert for å erstatte eller gjenopprette funksjonaliteten til et skjermingsverdig objekt.

Opplysninger om hendelser i fortid

Kategorien omfatter rapporter om sikkerhetsbrudd, rapporter som omhandler sikkerhetstruende virksomhet eller forsøk på sådan. Evalueringer av gjennomførte øvelser kan også ha et skadepotensial. I vurderinger av opplysninger som omhandler hendelser (eller fravær av hendelser) i fortid må virksomheten være oppmerksom på såkalte falske negativer, altså en opplysning om at en hendelse ikke har inntruffet, selv om den i realiteten har inntruffet. Eksempelvis er opplysningen «*Ingen uberettigede inntrengninger i datasystemet i 2018*» tilsynelatende en opplysning uten skadepotensial, og den skal dermed ikke sikkerhetsgraderes. Men i et tilfelle der en trusselaktør faktisk har gjennomført en inntrengning i det aktuelle datasystemet, så vil opplysningen avsløre at inntrengingen ikke ble oppdaget, og at virksomheten dermed har en manglende kapasitet til å oppdage den aktuelle typen inntrenginger i virksomhetens system.

Opplysninger om hendelser i fremtid

Kategorien omfatter hendelser som er planlagt eller er vurdert å kunne inntreffe i fremtiden, eksempelvis planlagte besøk. Øvelsesscenarioer kan også omfattes av denne kategorien.

Opplysninger om militære og sivile operasjoner

Kategorien omfatter opplysninger og vurderinger av planlagte eller gjennomførte operasjoner. I tillegg til militære og sivile operasjoner omfatter kategorien også sivil-militære operasjoner.

EOS-tjenestenes kilder og metoder

Kategorien omfatter opplysninger om hvordan tjenestenes produkter utarbeides og evalueres.

Spørsmål 3: Hva er opplysningens presisjonsnivå?

Presisjonsnivået i opplysningen kan i noen tilfeller være avgjørende for hvor stor skadefølgen kan bli ved tap av konfidensialitet. Som regel vil et høyere presisjonsnivå i opplysningen bety at mer kunnskap overføres til uvedkommende ved tap av konfidensialitet, og dermed kan en trusselaktørs kapasitet til å skade nasjonale sikkerhetsinteresser øke. Noen former for opplysninger med ulik grad av presisjonsnivå kan være:

- Opplysninger med tidsangivelse. Eksempelvis er «*i nær fremtid*» en mindre presis angivelse enn «*20. mars 2020*».
- Opplysninger med stedsangivelse. «*Munchs gate*» er en mer presis stedsangivelse enn «et sted i Oslo»

- Opplysninger om personer «*Ola Normann, født i 1975*» er en mer presis opplysning enn «*En mann i 40-årene*».

Opplysninger som sammenligner egenskaper eller tilstander ved ulike forhold kan også øke opplysningens presisjonsnivå. Slike opplysninger vil ofte bestå av gradsbøyde adjektiver. Positiver («*stor*», «*viktig*», «*rask*»), komparativer («*viktigere*», «*større*» «*mindre*», «*tidligere*») og superlativer («*raskest*», «*flest*», *færrest*») kan innebære at opplysningen får en merverdi gjennom å gradere eller rangere forhold. Særlig vil dette kunne gjelde for opplysninger i kategoriene skadevurderinger, sårbarhetsvurderinger, konsekvensvurderinger, trusselvurderinger, samt spesifikasjoner, kapasiteter og kapabiliteter. Eksempelvis vil det kunne være ulike skadepotensialer tilknyttet. Den første opplysningen kan ha et lavere skadepotensial enn de andre opplysningene i dette eksempelet:

- *«Datasystemene SH39 og D-ARA understøtter virksomhetens produksjon»*
- *«Datasystemene SH39 og D-ARA er **viktige** for virksomhetens produksjon»*
- *«Datasystemet SH39 er **viktigere** enn D-ARA for virksomhetens produksjon»*
- *«SH39 er det **viktigste** datasystemet for virksomhetens produksjon»*

Spørsmål 4: Øker sammenstillingen av opplysningene skadepotensialet?

Som hovedregel er det er den høyeste sikkerhetsgraden av enkeltopplysninger i en avgrenset informasjonsmengde som er førende for hvilken sikkerhetsgrad den samlede informasjonsmengden får. Sammenstilling av opplysninger kan likevel føre til at den samlede informasjonsmengden får en høyere verdi enn summen av enkeltopplysningene. Etter å ha vurdert alle opplysningene i en avgrenset informasjonsmengde opp mot de foregående spørsmålene må alle opplysningene ses i sammenheng. Det innebærer å vurdere om sammenstillingen av opplysningene gir et større skadepotensial enn det som er vurdert for de enkelte opplysninger.

- I noen tilfeller vil ikke sammenstillingen av opplysninger i en avgrenset informasjonsmengde øke informasjonsmengdens skadepotensial ut over det som er vurdert å gjelde for de enkelte opplysningene.
- I andre tilfeller kan en informasjonsmengdes skadepotensial variere i forholdsmessighet med antallet opplysninger som inngår i informasjonsmengden, og disses skadepotensial.

Selve sammenstillingen av opplysninger i en avgrenset informasjonsmengde kan også øke informasjonsmengdens skadepotensial. Dette ved at sammenstillingen avslører assosiasjoner eller sammenhenger som de enkelte opplysningene hver for seg ikke avslører, og der disse assosiasjonene eller sammenhengene i seg selv har et skadepotensial. Dette økte skadepotensialet kan oppstå i situasjoner der faktumet at opplysninger er relatert til hverandre, i seg selv har et skadepotensial. Det økte skadepotensialet kan også oppstå der to opplysninger satt i sammenheng avslører en implisitt opplysning med et større skadepotensial. Dette kan sammenlignes med følgende opplysninger: «*Mennesker er dødelige*» og «*Sokrates er et menneske*», hvorpå man kan resonnere seg frem til konklusjonen om at Sokrates er dødelig. Den som verdivurderer må derfor vurdere hvorvidt en sammenstilling gjør det mulig å «*lese mellom linjene»*.

Spørsmål 5: Kan en trusselaktør, dersom denne blir kjent med informasjonen, påføre nasjonale sikkerhetsinteresser skade?

Etter å ha vurdert hva informasjonen handler om, hvilke kategorier den inngår i, hvilket presisjonsnivå den har, og hvorvidt sammenstilling øker skadepotensialet, skal den som verdivurderer ha grunnlag til å beslutte hvorvidt informasjonen skal sikkerhetsgraderes, og eventuelt på hvilket nivå. Er svaret ***nei*** på spørsmålet om en trusselaktør som er kjent med informasjonen kan påføre nasjonale sikkerhetsinteresser, skal ikke informasjonen sikkerhetsgraderes. Er svaret imidlertid ***ja***, så må skadepotensialet vurderes opp mot formuleringene i SL § 5-3. Skadepotensial og NSMs forståelse av formuleringene tilknyttet de ulike sikkerhetsgradene er beskrevet i kap. 3 i NSMs veileder i verdivurdering av informasjon.

Til hjelp i vurderingen kan svarene i de foregående spørsmålene benyttes til å utforme en argumentasjonsrekke som underbygger følgende:

- ***Hvordan*** kan uvedkommende utnytte informasjonen?
- ***Kan*** det få skadefølger for nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommen
- ***I hvor stor grad*** kan det få skadefølger om informasjonen blir kjent for uvedkommende?

De ovennevnte vurderinger ender så med en formulering, som eksemplifisert under, som underbygger vurdering av at informasjonen må sikkerhetsgraderes.

«Informasjonen som verdivurderes omhandler beskrivelser av digitale sårbarheter i en infrastruktur som virksomheten råder over. Sårbarheten som beskrives kan utnyttes til å sette systemet ut av drift i en lengre periode. Presisjonsnivået i opplysningen kan sette en trusselaktør i stand til å effektivt gjøre dette. Den aktuelle infrastrukturen understøtter Forsvarets overvåking av norsk luftrom. Tap av konfidensialitet regnes derfor å kunne lede til svekkelse av Norges evne til suverenitetshevdelse. Opplysningen graderes derfor KONFIDENSIELT.»

Spørsmål 6: Hvor lenge har informasjonen behov for beskyttelse?

Sikkerhetsgraderingen skal ikke vare lengre enn nødvendig, jf. § 5-3.2.ledd. Den som verdivurderer må derfor vurdere hvorvidt beskyttelsesbehovet anses å opphøre på eller etter en spesifikk dato eller ved eller etter en hendelse. Om ikke den som verdivurderer kan fastsette et tidligere tidspunkt der beskyttelsesbehovet anses å opphøre er hovedregelen at sikkerhetsgraden bortfaller etter 30 år. Behov for beskyttelse som overskrider 30 år omtales på side 12 i veilederen.

Om beskyttelsessbehovet for informasjon opphører før tidspunktet for avgradering vil informasjonen være gjenstand for en omgradering. Det gjelder også for informasjon der beskyttelsesbehovet ikke opphører, men endres. Omgradering er omtalt på side 13 i veilederen.

Del 3. Beskyttelse av sikkerhetsgradert informasjon

Etter at virksomheten har vurdert og besluttet at en informasjonsmengde skal sikkerhetsgraderes, så er det siste steget i verdivurderingsprosessen å sørge for at beslutningen kommuniseres til brukerne av informasjonen, eksempelvis ved å merke informasjonen med korrekt sikkerhetsgrad.

For å forenkle håndtering, gjenbruk og beskyttelse av sikkerhetsgradert informasjon skal merkingen, så langt det er praktisk mulig, vise hvilke deler av en informasjonsmengde som har hvilken sikkerhetsgrad eller ingen sikkerhetsgrad. Det fullstendige dokumentet eller lagringsmediet skal graderes med minst den høyeste sikkerhetsgrad som er benyttet i dokumentet eller lagringsmediet.

Utforming og plassering av merking utdypes i NSMs veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon.

Virksomheten må gjennomføre de forebyggende sikkerhetstiltakene som må til for å oppnå forsvarlig sikkerhetsnivå for den spesifikke informasjonsmengden, samt alle andre skjermingsverdige verdier virksomheten råder over. Vurderinger og tiltak for forsvarlig sikkerhetsnivå omhandles i NSMs øvrige veiledere, håndbøker og tekniske råd. Foruten omgradering (omtalt i verdivurderingsveilederen) er det to forhold som kan følge i etterkant av beslutning om original sikkerhetsgradering, men som samtidig tilhører verdivurderingdisiplinen; reduksjon av skadepotensial, og utarbeidelse av retningslinjer for sikkerhetsgradering.

Reduksjon av skadepotensial

Virksomheten kan ha behov for å redusere skadepotensialet til opplysninger den har tilvirket. Dette kan være nødvendig dersom det er behov for å gjøre tilgjengelig eller distribuere hovedinnholdet i en informasjonsmengde, men at dette vanskeliggjøres ved at mulighetene for å beskytte denne ikke finnes i tilstrekkelig grad. Redusert skadepotensial kan oppnås gjennom tilsløring (anonymisering, noen ganger omtalt som *sanitisering)*, fjerning eller reduksjon av presisjonsnivå eller annen omskriving av opplysningene. Virksomheten må være særlig påpasselig med å sørge for at man oppnår en faktisk reduksjon av skadepotensial.

Utarbeidelse av retningslinjer for sikkerhetsgradering

Virksomhetens leder skal fastsette et styringsdokument som blant annet beskriver prinsipper for virksomhetens sikkerhetsarbeid (VF § 4, bokstav c). Virksomhetsinterne retningslinjer for sikkerhetsgradering av informasjon kan være en del av virksomhetens sikkerhetsprinsipper. Slike retningslinjer kan utformes som registre som inneholder virksomhetens beslutninger om sikkerhetsgradering av opplysninger som virksomheten har tilvirket. Hensikten er å ha kontroll over og kommunisere graderingsbestemmelser på en måte som legger til rette for at virksomhetens personell er konsekvente i anvendelsen av sikkerhetsgradering. Retningslinjene kan utvikles og vedlikeholdes løpende, etter hvert som det besluttes å sikkerhetsgradere nye typer opplysninger som virksomheten tilvirker. Alternativt kan virksomheten etablere spesifikke registre i forbindelse med etableringen av et nytt prosjekt, utføringen av en ny oppgave, eller oppsettet av et nytt system. For mange virksomheter kan egne retningslinjer for sikkerhetsgradering være et godt tiltak for å sørge for effektiv og konsekvent sikkerhetsgradering av informasjon som tilvirkes.

Gode registre vil hjelpe personellet med å fatte korrekte beslutninger om sikkerhetsgradering, effektivisere samarbeid og informasjonsdeling, og hjelpe med å beslutte hvilket informasjonssystem som skal benyttes i tilvirkningen av informasjonen. Gevinsten er redusert risiko for feilgradering. Retningslinjer er et hjelpemiddel, og ikke en erstatning av de individuelle verdivurderingene. Den som verdivurderer må fortsatt gjøre selvstendige vurderinger, men kan bruke retningslinjene som støtte til å fatte riktig beslutning om sikkerhetsgradering. I Tabell 1 følger et eksempel på et enkelt register.

Tabell 1 Register for sikkerhetsgradering av informasjon om Øvelse Panserbrett

Opplysning	**Sikkerhetsgrad**	**Årsak**	**Tidspunkt for avgradering**	**Deling**	**Kan opplysningen omtales på en ugradert måte?**
Opplysninger som bekrefter øvelsens eksistens	Ugradert	*Vurdering av skadepotensial*			
Opplysninger som bekrefter tidspunkt for øvelsen	Ugradert	*Vurdering av skadepotensial*			
Opplysninger som omhandler innholdet i øvelsens scenario	Ugradert	*Vurdering av skadepotensial*			
Opplysninger som bekrefter samtlige virksomheter som deltar i øvelsen	BEGRENSET	*Vurdering av skadepotensial*	5 år		«Øvelsen omfatter en rekke offentlige og private virksomheter»
Opplysninger om hvilken beredskapsplan som øves	BEGRENSET	*Vurdering av skadepotensial*	5 år	Deling utover virksomheter som deltar i øvelsen godkjennes i hvert enkelt tilfelle av øvelsens hovedplanlegger (OPR).	
Opplysninger som bekrefter samtlige virksomheter som deltar i øvelsen kombinert med hvilken beredskapsplan som øves	KONFIDENSIELT	*Vurdering av skadepotensial. Eks:* Det kan få skadefølger for nasjonale sikkerhetsinteresser om opplysningene blir kjent for uvedkommende. Dette fordi kombinasjonen av deltakelse (B), hvilken plan som øves (B), og scenarioet (U), gir en trusselaktør kunnskap som kan benyttes til å utarbeide mottiltak som reduserer beredskapstiltakenes effekt.	10 år	Deling utover virksomheter som deltar i øvelsen godkjennes i hvert enkelt tilfelle av øvelsens hovedplanlegger (OPR).	

Virksomheten kan utforme registre og oversikter slik den finner det hensiktsmessig. Nedenfor er forslag til noen rader som kan benyttes:

- Opprettelsesdato og/eller revisjonsdato
- Kontaktinformasjon ved spørsmål til retningslinjene
- Grunnlag for sikkerhetsgrad
- Dato/år for avgradering
- Dato/år for revidering

- Merknader ved spesielle/særskilte håndteringsforbehold
- Merknader om hvem informasjonen kan deles med

3. Referanser

US Department of Defence – Manual 5200.45 - Instructions for Developing Security Classification Guides https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520045m.pdf

ISOO (Information Security Oversight Office/US National Archives) - Developing and Using Security Classification Guides https://www.archives.gov/files/isoo/training/scg-handbook.pdf

Nasjonal sikkerhetsmyndighet - Veileder i verdivurdering av informasjon https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-verdivurdering-av-informasjon.pdf

Nasjonal sikkerhetsmyndighet – Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-handtering-og-beskyttelse-av-sikkerhetsgradert-informasjon.pdf

Nasjonal sikkerhetsmyndighet – Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/2019/veileder-i-departementenes-identifisering-av-gnf.pdf

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no