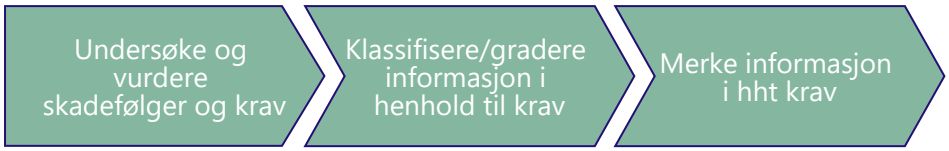
Verdivurdering av informasjon



Verdivurdering av informasjon

Prosesseier: Even Torp | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 12.4.2023 | Publisert versjon: 1

Hensikt:
Verdivurdering av informasjon handler om å vurdere hvor viktig informasjonen er for å oppfylle formålet med den, samt hvilket skadepotensial det ligger i at informasjonen blir kjent for uvedkommende, blir endret eller blir utilgjengelig.

Verdivurdering av informasjon er et nødvendig grunnlag for å kunne utøve god risikostyring og finne løsninger som bidrar til å unngå skader og tap. Ved manglende verdivurderinger av informasjon, eller feilvurdering av et informasjonsprodukts verdi, øker risikoen for at sentrale verdier havner i feil hender, blir endret eller utilgjengelig. For informasjon av betydning for nasjonale sikkerhetsinteresser kan det i verste fall påvirke rikets sikkerhet og befolkningens trygghet.

Omfang:
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 er skjermingsverdig etter sikkerhetsloven dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.
Informasjon er skjermingsverdig etter sikkerhetsloven dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

- Konfidensialitet (K)– ivareta konfidensialitet ved å unngå at informasjon blir kjent for uvedkommende.
- Integritet (I) – ivareta integritet ved å unngå at informasjon endres urettmessig eller utilsiktet.
- Tilgjengelighet (T) – ivareta tilgjengelighet ved å unngå at informasjon går tapt eller på annen måte gjøres utilgjengelig for rettmessige brukere.

Skjermingsverdig informasjon kan være gradert eller ugradert, og informasjonen kan lagres og formidles på flere måter.
All informasjon som kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig er skjermingsverdig etter sikkerhetsloven.
For skjermingsverdig informasjon som beskyttes av konfidensialitetshensyn, skal sikkerhetsgradering brukes. Graderingsnivåene er et uttrykk for skadepotensialet for nasjonale sikkerhetsinteresser, og dermed også beskyttelsesbehovet, dersom uvedkommende blir kjent med informasjonen.

For informasjon som er skjermingsverdig kun av integritets- eller tilgjengelighetshensyn, finnes det ikke et tilsvarende system med ulike graderingsnivåer for skadepotensial og beskyttelsesbehov. Slik informasjon kalles derfor skjermingsverdig ugradert informasjon. NND benytter definerte merkinger i sin kontorstøtteplattform (Office 365) for å merke skjermingsverdig ugradert informasjon.
Informasjon som ikke faller inn under beskrivelsene ovenfor verdivurderes som åpen, og merkes i henhold til dette.

Prosessen består av følgende vurderingspunkter:

- Vurdering av informasjonens betydning for nasjonale sikkerhetsinteresser (NSI).
- Vurdering av informasjonens skadepotensiale.
- Vurdering av konsekvenser ved sammenstilling av flere informasjonskilder.
- Endelig verdivurdering – Konfidensialitet (K), Integritet (I), Tilgjengelighet (T) med tilhørende merking.

Inngang:
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 evt. på hvilket nivå.
Fremgangsmåten innebærer både å vurdere opplysninger hver for seg, og som samlede informasjonsmengder. Sikkerhetsloven og forskriftenes bruk av begrepet informasjon legger til grunn en vid forståelse av hva begrepet kan omfatte. Måten informasjon er tilvirket på og hvilken form informasjonen har er ikke relevante momenter i vurderingen av om noe er å betrakte som informasjon. Begrepet omfatter for eksempel opplysninger gitt i fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger.

Resultat:
Verdivurderingen totalt sett vil gi svar på følgende:

- Har verdien interesse for uvedkommende? Hvorfor?
- Hvilke konsekvenser vil det få dersom verdien tilfaller uvedkommende, blir urettmessig endret eller blir gjort utilgjengelig?

Ved manglende kunnskap om verdivurdering kan man risikere å feilgradere informasjon. Å gi informasjon uriktig sikkerhetsgrad kan øke risiko for sikkerhetstruende virksomhet.

- For høy sikkerhetsgrad/«overgradering» vil gjerne medføre at NND bruker flere sikkerhetstiltak enn nødvendig, deriblant innen personellsikkerhet. Høyt gradert informasjon krever omfattende sikkerhetsklareringer og autorisasjoner for de ansatte som skal arbeide med informasjonen. I tillegg kan overgradering av informasjon også føre til at graderingsnivået ikke respekteres av virksomhetens ansatte. Dette er eksempler på risikostyring som er ineffektiv og uforholdsmessig inngripende for personer tiltakene omfatter, fordi sikkerhetstiltakene som iverksettes ikke står i forhold til verdien som skal beskyttes. Uriktig sikkerhetsgrad omtales ofte som en feilgradering.
- For lav sikkerhetsgrad/«undergradering» innebærer at NND ikke beskytter informasjonen på en forsvarlig måte, sett i lys av skadepotensialet informasjonen representerer. Dette kan forekomme i virksomheter som ønsker å unngå å måtte implementere omfattende sikkerhetstiltak. Dette er imidlertid å regne som et sikkerhetsbrudd. Feilgraderinger hvor informasjonen gis for lav sikkerhetsgrad kalles for undergradering.

I tillegg til feilgradering av informasjon som beskyttes av konfidensialitetshensyn, finnes det også eksempler på at unødvendig mye informasjon vurderes å være skjermingsverdig etter sikkerhetsloven (gradert eller ugradert). Et eksempel som man kan finne i norsk forvaltning er der «ubehagelige» opplysninger blir pekt på som skjermingsverdige. Dette trenger ikke nødvendigvis være fordi opplysningene har betydning for norske sikkerhetsinteresser (NSI), men fordi det er ønskelig at informasjonen holdes unna offentligheten av andre hensyn. Å gradere informasjon for å ivareta NND omdømme, er imidlertid ikke en gyldig grunn for graderingen.

Roller og rollenes ansvar i prosessen:

Utførende roller i prosessen	***Rollens oppgaveansvar/myndighet i denne prosessen***
Informasjonseier	Verdivurdere og merke informasjonen
Verdivurderer	Den som bidrar i arbeidet med å verdivurdere

Eksterne krav/føringer til prosessen:

Kravdokument (lovverk, standarder o.l.) kapittel, paragraf e.l.
Sikkerhetsloven §5-1. Skjermingsverdig informasjon
Virksomhetsikkerhetsforskriften § 22.Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon
Beskyttelsesinstruksen § 1. Anvendelse
Atomenergiloven § 53.(taushetsplikt)
Forvaltningsloven § 13 f.(bestemmelser om taushets- og opplysningsplikt m.m. i andre lover).
Offentleglova § 13.Opplysningar som er underlagde teieplikt
NSM- Veileder i verdivurdering av informasjon (eksternt dokument)
NSM - Håndbok i verdivurdering av informasjon (eksternt dokument)
NSM – Håndbok i skadevurdering
IAEA: NSS No. 23-G Security of Nuclear Information (spes. Kap 3 og 4, samt annex I og II)

Virksomhetskrav:

Kravdokument, kapittel, paragraf e.l.
Sikkerhetspolitikk
Politikk for informasjonssikkerhet
Delstrategi for dokumentforvaltning og verdivurdering
Instruks for forebyggende sikkerhet
Instruks for informasjonssikkerhet

Dokumentert informasjon (styrende dokumentasjon)

Veiledning

- Veileder for merking og håndtering av informasjon
- Veileder for verdivurdering av informasjon

Linker

Prosess - Forebyggende sikkerhet

Undersøke og vurdere skadefølger og krav

Prosesseier: Even Torp | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 25.4.2023 | Publisert versjon: 1

Inngang:

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.

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 opplysninger om temaet som tidligere er blitt publisert eller på annen måte er allment kjent.

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 og/eller betydning for NND. Det at informasjonen kan relateres til forhold av betydning for nasjonale sikkerhetsinteresser, er en forutsetning for å sikkerhetsgradere informasjon.

I sikkerhetsloven og virksomhetsikkerhetsforskriften er det også egne bestemmelser om verdivurdering ved anskaffelser. Ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur, skal oppdragsgiveren vurdere risikoen – en risikovurdering innebærer etter forskriften at også verdien skal inngå som en faktor i vurderingen.

Omfang/Aktiviteter:

Før selve verdivurderingen er det i dette prosessteget tre spørsmål om den som verdivurderer må ta stilling til:

a) Er opplysningen, eller tilsvarende opplysninger, vurdert 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. Hvis en informasjons-mengde utelukkende består av tidligere verdivurderte opplysninger, så kan den som verdivurderer gå videre til spørsmålet om sammenstilling (***spørsmål 4*** i selve verdivurderingen nedenfor).

b) Kan informasjonen kontrolleres?

NND må ha tillit til at konfidensialiteten til informasjon som sikkerhetsgraderes er ivaretatt, og at den kan ivaretas. Den som verdivurderer 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. NND 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.

c) Hvem er det informasjonen omhandler?

NND 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 NND som tilvirker av informasjonen vurdere å konsultere den andre virksomheten i løpet av verdivurderingsprosessen, eller på annen måte be om virksomhetens vurdering av opplysningene.

Videre i selve verdivurderingen må den som verdivurderer starter selve vurderingen med å ta stilling til hvorvidt opplysningen omhandler et forhold som er relatert til eller er av betydning for nasjonale sikkerhetsinteresser. Følgende spørsmål skal stilles og besvares:

Spørsmål 1: Omhandler opplysningen et forhold 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.

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.

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. Disse kategoriene, som beskrives nedenfor, har egenskaper som kan utnyttes til å forberede og gjennomføre sikkerhetstruende virksomhet, samt påvirke følgene av sikkerhetstruende virksomhet. 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 NND 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 NND 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**.**

- **Sårbarhetsvureringer**
  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 NNDs trusselbilde. Kategorien omfatter også vurderinger av trusselaktørers vilje til å utføre en handling, aktørens hensikt ved å utføre handlingen (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.
- **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. 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.

- **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 NNDs 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 IT-systemet i 2022» 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 IT-systemet, så vil opplysningen avsløre at inntrengingen ikke ble oppdaget, og at NND dermed har en manglende kapasitet til å oppdage den aktuelle typen inntrenginger i NNDs 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.
- **Etterretning-, overvåkings-, og sikkerhetstjenestenes (EOS) 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.

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.

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. Informasjonen skal da følge NND sin veileder for merking og behandling av ugradert informasjon.

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?

Spørsmål 6: Hvor lenge har informasjonen behov for beskyttelse?
For informasjons som skal sikkerhetsgraderes, skal ikke sikkerhetsgraderingen 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. Hovedregelen er at en sikkerhetsgradering bortfaller etter 30 år.

Spørsmål 7: Hva er konsekvensen ved brudd på informasjonens tilgjengelighet?
Hvor lenge kan informasjonen være utilgjengelig før det vil kunne påvirke NNDs drift eller egen sikkerhet eller interesser? Hvis f.eks. informasjon og informasjonssystemer hos NND som inneholder viktige planer, transportoversikter, beredskapslister og tilsvarende informasjon som er viktig for NNDs daglige virke blir

utilgjengelig. Vil risikoen for feil, mangler og problemer innen håndtering av nukleært materiale, reaktorer og atomanlegg kunne øke.

Spørsmål 8: Hva er konsekvensen av brudd på informasjonens integritet?
Hvis informasjonen endres, slik at den ikke er korrekt, gyldig eller fullstendig, vil det kunne påvirke NNDs drift eller egen sikkerhet? Endringer av data eller funksjoner i viktige informasjonssystemer som potensielt kan gi feil ved styring kan igjen skape ulykker.

Resultat:
De ovennevnte vurderinger ender så med en formulering, som eksemplifisert nedenfor, som underbygger vurdering av at informasjonen må sikkerhetsgraderes eller om den skal merkes og behandles som ugradert men skjermingsverdig.

«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.»

Dokumenter som er nødvendig for denne prosessen:

NSM- Veileder i verdivurdering av informasjon (eksternt dokument)
NSM - Håndbok i verdivurdering av informasjon (eksternt dokument)
NSM – Håndbok i skadevurdering

Klassifisere/gradere informasjon i henhold til krav

Prosesseier: Even Torp | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 25.4.2023 | Publisert versjon: 1

Inngang:

Basert på verdivurderingen i forrige prosessteg skal du ha fått tilstrekkelig grunnlag til å kunne klassifisere/gradere informasjonen i henhold til relevante krav.

Som hovedregel skal informasjon som kan utløse et objekts skadepotensial sikkerhetsgraderes i henhold til alvorlighetsgraden til skadepotensialet og evt. klassifiseringsnivå.

Omfang/Aktiviteter:

Gjør nå en vurdering av mulig graderingsspesifikasjon for å angi hvilken gradering informasjonen skal ha. Alle dokumenttyper og øvrig informasjon skal vurderes ut i fra når de produseres av tilvirker. Hensikten med en graderingsspesifikasjon er å tydeliggjøre hvilken informasjon som er skjermingsverdig samt etablere et nivå for sikkerhetstiltak gjennom gradering. Hovedprinsippene for vurdering av skjermingsnivå er etablert gjennom informasjonens skadepotensiale.

Informasjon som skal graderes i henhold til sikkerhetsloven skal omfatte forhold som kan knyttes til nasjonale sikkerhetsinteresser (NSI) og/eller grunnleggende nasjonale funksjoner (GNF). Informasjon som av andre grunner enn skjerming ved sikkerhetsgradering i henhold til sikkerhetsloven, skal beskyttelsesgraderes etter andre bestemmelser og lovverk.

Formuleringen i sikkerhetslovens §5-3 «*(…) dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende»* omhandles som skadepotensiale. Her legges det til grunn at vurderingen av skadepotensialet er en vurdering av hvorvidt, og i hvor stor grad,tap av konfidensialitet kan føre til *svekkelse, forringelse* eller *forhindring* av nasjonale sikkerhetsinteresser. Følgende er en ikke uttømmende oversikt over kategorier av informasjon som kan ha et skadepotensial:

- Skadevurderinger
- Sårbarhetsvurderinger
- Konsekvensvurderinger
- Trusselvurderinger
- Etterretning
- Opplysninger om spesifikasjoner, kapasiteter og kapabiliteter (evner)
- Opplysninger om kryptologi
- 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)

Hvorvidt slike opplysninger faktisk har et skadepotensial avhenger av grad av kobling av informasjonen har til de nasjonale sikkerhetsinteressene, og informasjonen har et prisisjonsnivå.

Dersom informasjonen som tilvirkes kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende skal følgende sikkerhetsgrader benyttes:

1. STRENG HEMMELIG – dersom det kan få helt avgjørende skadefølger
2. HEMMELIG – dersom det kan få alvorlige skadefølger
3. KONFIDENSIELT – dersom det kan få skadefølger
4. BEGRENSET – dersom det i noen grad kan få skadefølger

I sikkerhetsloven er det et system med tre klassifiseringsgrader for objekt og infrastruktur (SL § 7-2). Klassifiseringsnivåene er et uttrykk for skadepotensialet dersom objektet eller infrastrukturen får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse:

- Dersom det kan få helt avgjørende skadefølger: MEGET KRITISK
- Dersom det kan få alvorlige skadefølger: KRITISK
- Dersom det kan få skadefølger: VIKTIG

For enkelte typer informasjon om objekter eller infrastrukturer, er det i regelverket gitt eksplisitte krav til graderingsnivået:

- Klassifiseringsnivået og grunnlaget for klassifiseringen skal graderes BEGRENSET eller høyere.
- En skadevurdering skal graderes BEGRENSET eller høyere.
- En oversikt over alle eller et større antall klassifiserte objekter eller infrastrukturer skal graderes KONFIDENSIELT eller høyere.

Selv om det ikke er nevnt eksplisitt i regelverket kan noe informasjon om et objekt eller infrastruktur måtte sikkerhetsgraderes fordi informasjonen kan lette planlegging og gjennomføring av angrep mot objektet eller infrastrukturen, f.eks.:

- Informasjon om sikkerhetstiltak
- Informasjon om sårbarheter
- Beredskapsplanverk

Slik informasjon kan gis et graderingsnivå som er lavere eller like høyt (men ikke høyere) som det korresponderende klassifiseringsnivået for objektet eller infrastrukturen:

- MEGET KRITISK = STRENGT HEMMELIG eller lavere
- KRITISK = HEMMELIG eller lavere
- VIKTIG = KONFIDENSIELT eller lavere

Det kan være enkelte unntak der hvor informasjon om et objekt/infrastruktur må graderes høyere enn klassifiseringsnivået tilsier. Dette kan typisk være der et dokument inneholder informasjon om forhold som graderes høyere av andre hensyn enn klassifiseringen av objektet/infrastrukturen.

Resultat:
Etter å ha vurdert om informasjonen kan ha betydning for NSI, skadefølger og hvorvidt presisjonsnivået eller sammenstilling av informasjon øker skadepotensialet, skal den som verdivurderer ha grunnlag for å beslutte hvorvidt informasjonen har potensiale til å påføre skade på NSI gjennom å ramme virksomheten

Merke informasjon i hht krav

Prosesseier: Even Torp | Godkjent av: Ann-Cathrin Becken | Godkjent dato: 25.4.2023 | Publisert versjon: 1

Inngang:

Etter en fullført verdivurdering og vurdering av skadeomfanget, vet du om informasjonen

1. er skjermingsverdig informasjon som av konfidensialitetshensyn skal merkes med riktig sikkerhetsgrad etter sikkerhetsloven, og beskyttes deretter.
2. er skjermingsverdig informasjon som av integritets- og/eller tilgjengelighetshensyn skal beskyttes deretter.
3. ikke er skjermingsverdig informasjon etter sikkerhetsloven.

Det er virksomheten som tilvirker informasjon og er ansvarlig for å verdivurdere den, som også er ansvarlig for å merke informasjonen med riktig graderingsnivå.

Omfang/Aktiviteter:

Informasjon som «kun» er skjermingsverdig, men ikke sikkerhetsgradert, skal merkes i henhold til veilederen for merking og håndtering av ugradert informasjon.

For sikkerhetsgradert informasjon er det krav til merking. Her følger du instruksen for merking og håndtering av gradert informasjon.

Dokumenter og lagringsmedier skal merkes med den høyeste sikkerhetsgraden som gjelder informasjon o dokumentet eller lagringsmediet, og med hvor lenge graderingen varer. Merkingen skal være lett synlig og lett kunne gjøres kjent for alle i og utenfor NND som skal håndtere informasjonen.

I tilfeller hvor ikke all informasjon i et dokument eller et lagringsmedium har samme sikkerhetsgradering, skal merkingen, så langt det er praktisk mulig, vise hvilke deler som har hvilken gradering eller ingen gradering. Dette kan f.eks. gjøres med forkortelsen U (for ugradert) og B, K, H eller SH (for respektive graderingsnivå) foran en overskrift eller et avsnitt. Hvis det er noen få opplysninger som må graderes høyere enn resten, kan denne informasjonen plasseres i eget (egne) vedlegg med annen gradering.

Resultat:

Når NND håndterer en risiko knyttet til skjermingsverdig ugradert informasjon skal tiltakene som et minimum sørge for at informasjonen ikke kan gå tapt, endres eller gjøres utilgjengelig med enkle midler. Dersom risikoen tilsier det, skal informasjonen også beskyttes mot avanserte angrepsmetoder. Ved vurdering av risikoen skal virksomheten ta hensyn til betydningen av virksomhetens skjermingsverdige verdier.

Konfidensialitet	Skjermingsverdig informasjon	BEGRENSET KONFIDENSIELT HEMMELIG STRENGT HEMMELIG	Merkes med gradering
Integritet	Skjermingsverdig informasjon	Ugradert	Ingen krav til merking, men virksomheten står fritt til internt å merke som skjermingsverdig ugradert informasjon.
Tilgjengelighet	Skjermingsverdig informasjon	Ugradert	Ingen krav til merking, men virksomheten står fritt til internt å merke som skjermingsverdig ugradert informasjon.

Etter å ha fullført prosessen *Verdivurdering av informasjon* er informasjonen verdivurdert og merket i hehold til gjeldende krav.

NND Styrende dokumenter under utarbeidelse:

Kommende tittel i Kjernen
Prosedyre for behandling av sikkerhetsgradert informasjon

Dokumentert informasjon (styrende dokumentasjon)

Veiledning

Veileder for merking og håndtering av informasjon