

Veileder fra NSM

Veileder i sikkerhetsgradert informasjon

Veileder fra NSM

Veileder i sikkerhetsgradert informasjon

Versjon	Godkjent dato	Dokumentnr	Sak
1.0	02.06.2025	U-25-79	U-25/00640

Siste versjon endret

Dato: 27.05.2025

Kun henvisninger/referanser Kun språklige endringer Endring i faglig innhold

Nasjonal sikkerhetsmyndighet (NSM) er sikkerhetsmyndighet etter lov om nasjonal sikkerhet (sikkerhetsloven) og fagorgan for forebyggende sikkerhet. NSM gir informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav til tiltak.

NSM har tre kategorier av veiledere.

- Veiledere lov og forskrift
- Håndbøker
- Tekniske veiledere

Veilederne representerer NSMs syn på hvordan lover og forskrifter er å forstå. De utdyper krav og gir tekniske og prosedyremessige anbefalinger. Veiledere legges til grunn for NSMs arbeid knyttet til godkjenninger og tilsyn. NSM tilbyr også kurs på sentrale områder, både som e-læring og fysiske kurs. Mer informasjon finnes på NSMs nettsider.

Vi anbefaler at NSMs ulike veiledninger leses i sammenheng for å sikre en helhetlig tilnærming til forebyggende sikkerhetsarbeid.

Ugraderte veiledere er åpent tilgjengelige på NSMs nettsider. Graderte veiledere er tilgjengelige på graderte samhandlingsplattformer og kan formidles fra NSM iht. tjenstlige behov.

NSM oppdaterer jevnlig dokumentene. Siste versjon av ugraderte veiledere er alltid tilgjengelig på NSMs nettsider.

NSMs veiledere er dokumenter som er ment å gi støtte til offentlige og private virksomheters arbeid med forebyggende sikkerhet. Virksomheter som er omfattet av sikkerhetsloven skal ha nødvendig informasjon om hvordan de kan oppnå forsvarlig sikkerhet

NSM utgir også andre publikasjoner av mer generell karakter, som ikke har status som veiledere, eksempelvis generelle grunnprinsipper for sikkerhet og andre rådgivende dokumenter.

Vi håper veilederne gir god støtte til arbeidet med forebyggende sikkerhet og mottar gjerne tilbakemeldinger dersom det er behov for endringer eller andre veiledere.

Innhold

Innhold	3
1. Tema for veilederen	4
2. Sikkerhetsgradert informasjon	4
2.1 Tilgjengelighet, integritet og konfidensialitet	5
3. Sikkerhetsgradering	6
3.1 Skadepotensial	7
3.2 Sammenstilling av informasjon	9
3.3. Graderingsnivåene	9
3.3.1 STRENGT HEMMELIG	9
3.3.2 HEMMELIG	10
3.3.3 KONFIDENSIELT	10
3.3.4 BEGRENSET	11
4. Endring av sikkerhetsgradering	11
4.1 Avgradering	12

1. Tema for veilederen

Veilederen gir en innføring i når informasjon skal sikkerhetsgraderes etter sikkerhetsloven. Formålet er å øke bevisstheten knyttet til at informasjon kan ha et skadepotensiale for nasjonale sikkerhetsinteresser, og øke forståelsen for hvorfor vi må beskytte denne type informasjon. Veilederen gir innsikt i forskjellen mellom skadefølger på de ulike sikkerhetsgraderingsnivåene, slik at informasjon kan sikres etter faktisk behov.

Aktuelle bestemmelser fremgår av sikkerhetsloven (sikkel) kapittel 5 og virksomhetsikkerhetsforskriften kapittel 5.

Det anbefales å se veilederen i sammenheng med annet veiledningsmateriale Nasjonal sikkerhetsmyndighet (NSM) har utarbeidet, blant annet håndbok i verdivurdering og håndbok i håndtering og beskyttelse av informasjon. Det vil også være hensiktsmessig å se veilederen i kontekst av de årlige trussel- og risikovurderingene som utgis av Politiets sikkerhetstjeneste, Etterretningstjenesten og NSM.

Veilederen vil være relevant for alle virksomheter som er underlagt sikkerhetsloven og som tilvirker, håndterer eller på annen måte har tilgang til skjermingsverdig og sikkerhetsgradert informasjon. Den vil ha særlig relevans for virksomheter som selv tilvirker slik informasjon.

For veiledning knyttet til annen informasjon som omfattes av og skal beskyttes etter sikkerhetsloven vises det til NSMs veileder for ugradert skjermingsverdig informasjon og informasjonssystem.

2. Sikkerhetsgradert informasjon

Sikkerhetsloven legger til grunn en vid forståelse av hva informasjon kan omfatte. Måten informasjon er tilvirket på og i hvilket format informasjonen kommer i, har ikke betydning for om det er å anse som informasjon. Begrepet omfatter for eksempel opplysninger gitt i fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger.

Informasjon må beskyttes etter sikkerhetsloven dersom det kan skade nasjonale sikkerhetsinteresser¹ om informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.² Sikkerhetsgradert informasjon er informasjon som kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende.³ Det er kun behovet for konfidensialitet som får betydning for om informasjonen skal sikkerhetsgraderes og beskyttes etter sikkerhetsloven.

Selv om det er et grunnleggende prinsipp i det norske demokrati å tilstrebe mest mulig åpenhet i forvaltningen, så vil det til enhver tid være informasjon som har et konfidensialitetsbehov. Informasjon som må hemmeligholdes av hensyn til nasjonale sikkerhetsinteresser kan være informasjon som gir nasjonen en fordel i forholdet til en

¹ Jf. sikk. § 1-5 nr. 1

² Jf. sikk. § 5-1

³ Jf. sikk. § 5-3

motpart, og/eller gir en motpart en fordel som kan skade nasjonen. Førstnevnte kategori kan eksempelvis være informasjon som omhandler våpenteknologi eller diplomatiske aktiviteter. Sistnevnte kategori kan blant annet knytte seg til beredskapsplanverk eller informasjon om Forsvarets kapabiliteter.

2.1 Tilgjengelighet, integritet og konfidensialitet

Som nevnt er det kun konfidensialitetsaspektet som har betydning for om informasjon skal sikkerhetsgraderes. Det kan imidlertid også være et behov for at informasjonens tilgjengelighet og integritet ivaretas, selv om det ikke begrunner sikkerhetsgradering. Det er derfor nyttig å forstå samspillet mellom disse.

- Dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, må informasjonens konfidensialitet beskyttes. Med konfidensialitet menes at informasjonen kun skal gjøres tilgjengelig for personer med nødvendig autorisasjon og som har tjenstlig behov for tilgang. Konfidensialitetsbeskyttelse innebærer beskyttelse mot uautorisert tilgang og offentliggjøring.
- Dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at informasjonen går tapt eller blir utilgjengelig, så må informasjonens tilgjengelighet beskyttes. Med tilgjengelighet menes at informasjonen er tilgjengelig for virksomheten innenfor det tidsrommet som virksomheten har behov for å bruke den. Dersom slik informasjon går tapt, eller blir gjort utilgjengelig, anses det som et tilgjengelighetsbrudd. Virksomheten må vurdere tilgjengelighetsbehovene til informasjonen den besitter, og identifisere konsekvenser for nasjonale sikkerhetsinteresser dersom informasjonen ikke er tilgjengelig for de riktige brukerne eller systemene til rett tid.
- Dersom det kan få skadefølger for nasjonale sikkerhetsinteresser at informasjonen blir endret, så må informasjonens integritet beskyttes. Med integritet menes at informasjonen er korrekt og fullstendig sett i sammenheng med emnet og omfanget som informasjonen har til hensikt å omfatte. Integritetsbeskyttelse innebærer å sørge for at det ikke lar seg gjøre urettmessig å endre innholdet i informasjonen.

Konfidensialitet, integritet og tilgjengelighet er ikke motsetninger. Tilgjengelighet må ikke forveksles med prinsippet om meroffentlighet, og er ikke en motpol til konfidensialitet. I mange tilfeller kan det være behov for å ivareta både konfidensialiteten, integriteten og tilgjengeligheten til en informasjonsmengde. Nasjonale beredskapsplaner er et eksempel på dokumenter med informasjon der alle tre aspektene må ivaretas. Om opplysningene i planene er kjent for en trusselaktør, kan de lett bli mindre effektive. Integriteten må ivaretas slik at man kan stole på at opplysningene i planene er korrekte. Tilgjengeligheten må også ivaretas slik at de som skal iverksette tiltak har planene for hånden når situasjonen krever det.

I andre tilfeller vil informasjonen ha et større tilgjengelighets- og integritetsbehov enn et konfidensialitetsbehov. Et eksempel kan være informasjon en flygeleder må ha tilgang til for å overvåke og dirigere sivil flytrafikk. Flygelederen har som hovedoppgave å forhindre sammenstøt av fly i luften eller på bakken, og for å sørge for rask og effektiv trafikkavvikling. Flygelederens oppgaveløsning er avhengig av en uavbrutt strøm av korrekte opplysninger fra

radar- og kommunikasjonssystemer. Dette er for å ha et oppdatert situasjonsbilde av hvilke fly som befinner seg i luftrommet, og hvor de befinner seg i forhold til hverandre. Informasjonens tilgjengelighet og integritet er derfor avgjørende for flygelederens evne til å løse sin oppgave. For flygelederens oppgaveløsning vil ikke ivaretagelse av konfidensialitet være det sentrale. Det betyr ikke at informasjonen likevel ikke kan ha et konfidensialitetsbehov i andre situasjoner eller for andre involverte aktører.

Informasjonens skjermingsbehov og forholdet mellom konfidensialitet, integritet, og tilgjengelighet kan endres etter omstendighetene. Det kan blant annet skyldes endringer i geo- eller sikkerhetspolitisk situasjon, men også pågående sikkerhetstruende virksomhet. Virksomheten må derfor fortløpende ta stilling til hvilket behov som totalt sett er viktigst å ivareta av hensyn til nasjonale sikkerhetsinteresser. Det vises til at det har betydning for hvilke krav som stilles til beskyttelse av informasjonen.

3. Sikkerhetsgradering

Det er virksomheten som tilvirker informasjonen som er ansvarlig for å vurdere hvorvidt informasjonen skal sikkerhetsgraderes, og på hvilket graderingsnivå. Sikkerhetsgradert informasjon skal sikkerhetsgraderes ut i fra hvilke skadefølger det kan få for nasjonale sikkerhetsinteresser:

- STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger
- HEMMELIG dersom det kan få alvorlige skadefølger
- KONFIDENSIELT dersom det kan få skadefølger
- BEGRENSET dersom det i noen grad kan få skadefølger

I vurderingen av om informasjon skal sikkerhetsgraderes må tilvirker kunne identifisere og beskrive potensielle skadefølger for nasjonale sikkerhetsinteresser ved konfidensialitetsbrudd. Det stilles ikke krav om at tap av konfidensialitet beviselig vil medføre skade, det er tilstrekkelig at det kan medføre skadefølger. Vurderingen kan imidlertid ikke basere seg på urealistiske antagelser. Sikkerhetstiltak etter sikkerhetsloven skal gjennomføres i samsvar med grunnleggende rettsprinsipper og det skal ikke iverksettes mer omfattende og inngripende sikkerhetstiltak enn det som er nødvendig.⁴ Sikkerhetsgradering av informasjonen medfører blant annet krav om autorisasjon og/eller sikkerhetsklarering for tilgang. Sikkerhetsklarering er et inngripende tiltak og skal ikke benyttes uten at det foreligger et faktisk behov. Det legger dermed føringer for vurderingen av om og på hvilket nivå informasjon skal sikkerhetsgraderes.

Dersom ikke all informasjon i et dokument eller i et lagringsmedium har samme sikkerhetsgrad, skal merkingen så langt det er praktisk mulig vise hvilke deler som har hvilken sikkerhetsgrad eller ingen sikkerhetsgrad.⁵ Dette kalles å punktgradere informasjon. Det fullstendige dokumentet eller lagringsmediet skal graderes med minst den høyeste sikkerhetsgrad som er benyttet i dokumentet eller lagringsmediet. Punktgradering kan

⁴ Jf. sikk. § 1-1 bokstav c, jf. virksomhetsikkerhetsforskriften § 15 tredje ledd, jf. sikk. § 5-3 annet ledd.

⁵ Jf. virksomhetsikkerhetsforskriften § 28.

forenkle håndteringen av sikkerhetsgradert informasjon ved at det blir enklere å dele informasjon til brukere med ulikt informasjonsbehov og autorisasjons- og klareringsnivå, i tillegg til at det forenkler gjenbruk av informasjonen.

I vurderingen av om informasjon skal sikkerhetsgraderes må det også tas stilling til hvor lenge konfidensialitetsbehovet vil gjøre seg gjeldende. I noen tilfeller vil det være mulig å fastsette et spesifikt tidspunkt hvor informasjonens konfidensialitetsbehov endres eller opphører. Det kan eksempelvis være informasjon som omhandler planverk, besøk eller øvelser, som ikke har et konfidensialitetsbehov etter at aktiviteten er gjennomført. Se punkt 4 for nærmere krav til av- og omgradering.

Det stilles ikke krav om skriftliggjøring av begrunnelsen for at informasjon skal sikkerhetsgraderes. Det kan imidlertid være fornuftig å sikre etterprøvbarhet for vurderingen, eksempelvis ved forespørsel om innsyn, deling eller om-/avgradering.

3.1 Skadepotensial

Vurderingen av skadepotensial er en vurdering av hvorvidt, og i hvor stor grad, tap av konfidensialitet kan føre til svekkelse, forringelse eller forhindring av nasjonale sikkerhetsinteresser. Følgende liste er en ikke-uttømmende oversikt over kategorier av informasjon som kan ha et skadepotensial for nasjonale sikkerhetsinteresser:

- Skadevurderinger
- Sårbarhetsvurderinger
- Konsekvensvurderinger
- Trusselvurderinger
- Etterretning
- Sivilt- og militært beredskapsplanverk
- Opplysninger om spesifikasjoner, kapasiteter og kapabiliteter
- Opplysninger om kryptologi
- 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
- EOS-tjenestenes kilder og metoder

Hvorvidt slike opplysninger faktisk har et skadepotensial avhenger av hvilken grad av kobling informasjonen har til nasjonale sikkerhetsinteresser, og informasjonens presisjonsnivå. Med grad av kobling menes hvor stor betydning forholdet som opplysningen omhandler har for nasjonale sikkerhetsinteresser. Eksempelvis har planverkene for nasjonal beredskap og krisehåndtering høy grad av kobling til de nasjonale sikkerhetsinteressene.

3.2 Sammenstilling av informasjon

Sammenstilling av opplysninger kan føre til at den samlede informasjonsmengden får et høyere skadepotensial enn det enkeltopplysningene vil ha. Det må derfor gjennomføres en vurdering av den samlede informasjonsmengden og hvilket skadepotensial det kan ha for nasjonale sikkerhetsinteresser. Dersom ny informasjon tilføyes utløser det behov for ny vurdering av informasjonens skadepotensial.

En sammenstilling av ugraderte opplysninger skal sikkerhetsgraderes om sammenstillingen avslører relasjoner som ikke på annen måte er avslørt i de individuelle opplysningene, og som kan ha et skadepotensial for nasjonale sikkerhetsinteresser.

Tilsvarende kan en sammenstilling av lavere gradert informasjon medføre at sammenstillingen må graderes på et høyere nivå. Som eksempel skal informasjon om klassifiseringsnivå for skjermingsverdige objekter og infrastruktur sikkerhetsgraderes som BEGRENSET eller høyere. En oversikt over samtlige eller et større antall klassifiserte objekter og infrastrukturer skal derimot sikkerhetsgraderes KONFIDENSIELT eller høyere.

3.3. Graderingsnivåene

I det følgende gis det eksempler på hva som omfattes av skadepotensial for de ulike sikkerhetsgraderingsnivåene, og hvilken terskel som må legges til grunn.

3.3.1 STRENGT HEMMELIG

Under følger en oversikt over hva som ligger i at konfidensialitetsbrudd kan få *helt avgjørende skadefølger* for nasjonale sikkerhetsinteresser:

- Bortfall eller svært kraftig svekkelse av regjeringens, Stortingets eller Høyesteretts funksjonsevne
- Bortfall eller svært kraftig svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Bortfall eller svært kraftig svekkelse av Norges evne til suverenitetshevdelse
- Bortfall eller svært kraftig svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Bortfall eller svært kraftig svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Stans av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Ødeleggelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Helt avgjørende skadefølger for allierte staters sikkerhet
- Stans av en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Bortfall eller svært kraftig svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Bortfall eller svært kraftig svekkelse av stabile kapitalforhold overfor utlandet
- Bortfall eller svært kraftig svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene

- Bortfall eller svært kraftig svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas

3.3.2 HEMMELIG

Under følger eksempler på hva som ligger i at konfidensialitetsbrudd kan få *alvorlige skadefølger* for nasjonale sikkerhetsinteresser:

- Kraftig svekkelse av regjeringens, Stortingets eller Høyesteretts funksjonsevne
- Kraftig svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Kraftig svekkelse av Norges evne til suverenitetshevdelse
- Kraftig svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Kraftig svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Kraftig forhindring av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Kraftig forringelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Alvorlige skadefølger for allierte staters sikkerhet
- Kraftig forhindring en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Kraftig svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Kraftig svekkelse av stabile kapitalforhold overfor utlandet
- Kraftig svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
- Kraftig svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

3.3.3 KONFIDENSIELT

Under følger eksempler på hva som ligger i at konfidensialitetsbrudd kan få *skadefølger* for nasjonale sikkerhetsinteresser:

- Svekkelse av regjeringens, Stortingets eller Høyesteretts funksjonsevne
- Svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Svekkelse av Norges evne til suverenitetshevdelse
- Svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Forhindring av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Forringelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- Skadefølger for allierte staters sikkerhet
- Forhindring av en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting

- Svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Svekkelse av stabile kapitalforhold overfor utlandet
- Svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
- Svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

3.3.4 BEGRENSET

Under følger eksempler på hva som ligger i at konfidensialitetsbrudd i *noen grad kan få skadefølger* for nasjonale sikkerhetsinteresser:

- Noe svekkelse av regjeringens, Stortingets eller Høyesteretts funksjonsevne
- Noe svekkelse av funksjonsevnen til prioriterte deler av forvaltningen
- Noe svekkelse av Norges evne til suverenitetshevdelse
- Noe svekkelse av evne til å opprettholde nasjonal beredskap og krisehåndtering
- Noe svekkelse av evne til å håndtere sikkerhetspolitiske kriser og forsvar av norsk territorium
- Noe forhindring av bilateralt samarbeid om sikkerhet og etterretning, inkl. deltakelse i internasjonale operasjoner
- Noe forringelse av samarbeidsrelasjoner med andre land og internasjonale organisasjoner (NATO, EU) om statssikkerhet
- I noen grad skadefølger for allierte staters sikkerhet
- Noe forhindring av en stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting
- Noe svekkelse av velfungerende systemer for å håndtere offentlige ytelser og inntekter
- Noe svekkelse av stabile kapitalforhold overfor utlandet
- Noe svekkelse av stabilitet i finansiell infrastruktur og i finansmarkedene
- Noe svekkelse av infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas.

4. Endring av sikkerhetsgradering

Omgradering innebærer å fastsette en annen sikkerhetsgradering både på høyere og lavere nivå, avgradere informasjonen, eller justere hvor lenge det er behov for å beskytte informasjon. Hovedregelen er at det er virksomheten som har tilvirket og sikkerhetsgradert informasjonen som skal vurdere og beslutte en eventuell omgradering av informasjonen.⁶

En overordnet virksomhet, ansvarlig sektordepartement og Nasjonal sikkerhetsmyndighet har også anledning til å omgradere sikkerhetsgradert informasjon. I tilfeller hvor det er uenighet om omgradering legges det til grunn at overordnet virksomhet og sektordepartement kan, innenfor sin alminnelige instruksjonsmyndighet, instruere underordnet virksomhet til å omgradere. NSM vil kunne benytte sin myndighet til å overprøve beslutninger

⁶ Jf. virksomhetsikkerhetsforskriften § 31, jf. § 33 annet ledd.

om omgradering ved åpenbare feilvurderinger som kan resultere i skadefølger for nasjonale sikkerhetsinteresser.

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 ulike opplysninger med ulike utstedende virksomheter, må det klart kunne identifiseres hvem som er informasjonseier av de enkelte delene.

Omgradering av sikkerhetsgradert informasjon skal vurderes i følgende tilfeller:

- Ved varsel om mulig feilgradering
- Ved henvendelse om innsyn i sikkerhetsgradert informasjon
- Ved avlevering av dokumenter til Arkivverket
- Dersom det av andre grunner er grunn til å tro at beskyttelsesbehovet for informasjonen har endret seg

4.1 Avgradering

Informasjon skal ikke sikkerhetsgraderes for en lengre periode enn det som er nødvendig. Dersom ikke annet er bestemt, bortfaller sikkerhetsgraderingen etter 30 år.⁷ Etter 30 år skal avgradering vurderes hvert tiende år.⁸

⁷ Jf. sikkl. § 5-3 annet ledd

⁸ Jf. virksomhetsikkerhetsforskriften § 29.

NSM

Nasjonal sikkerhetsmyndighet

Postboks 814

1306 Sandvika

postmottak@nsm.no

nsm.no