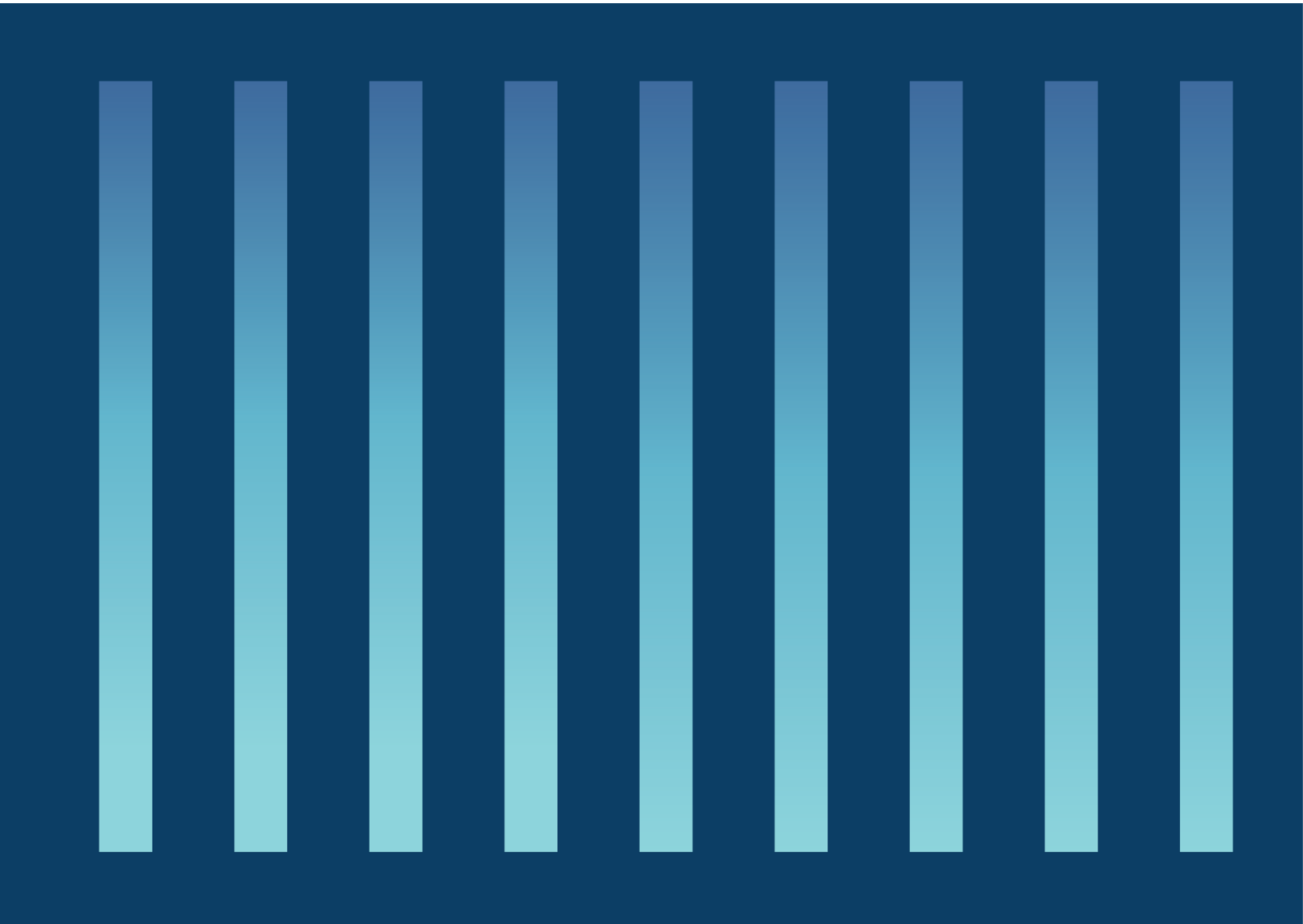
NASJONAL
SIKKERHETSMYNDIGHET

Veileder for godkjenning av informasjonssystem

Versjon: 3



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 veiledninger utdyper regelverkforståelsen, herunder den tematiske sammenhengen mellom ulike bestemmelser i sikkerhetsloven og tilhørende forskrifter. Veilederne representerer NSMs syn på hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket.

NSM gir i tillegg ut håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen.

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

INNHOLD

1. Sikkerhetsgodkjenning 3
1.1. Krav om sikkerhetsgodkjenning 3
1.2. Skjermingsverdige informasjonssystemer 4
1.3. Sikkerhetsgodkjenning ved sammenkobling 5
1.4. Godkjenningsmyndighet 7
1.5. Sikkerhetsgodkjenningens varighet 8
1.6. Midlertidig brukstillatelse 9
1.7. Fakturering 10
2. Grunnlag for sikkerhetsgodkjenning 11
2.1. Krav om forsvarlig sikkerhetsnivå 11
2.2. Krav til sikkerhetsgodkjenning 12
2.2.1. Funksjon og operativt miljø (systembeskrivelse) 13
2.2.2. Beskyttelsesbehov 14
2.2.3. Sikkerhetstiltak 15
2.2.4. Kontroll av sikkerhetstiltak 21
2.3. Evaluering av produkter og tjenester 21
Vedlegg 1 – Sikkerhetsgodkjenning som en del av utviklingsprosess 23
Vedlegg 2 – Eksempler på underlag for sikkerhetsgodkjenning 24

1. Sikkerhetsgodkjenning

Målgruppen for Veileder for godkjenning av informasjonssystem er virksomheter underlagt sikkerhetsloven og som har informasjonssystemer som må sikkerhetsgodkjennes, altså personell som skal forestå søknader om sikkerhetsgodkjenning og personell som skal forestå virksomhetens interne sikkerhetsgodkjenninger.

Skjermingsverdige informasjonssystemer er systemer for behandling av skjermingsverdig informasjon eller systemer som i seg selv er avgjørende for grunnleggende nasjonale funksjoner. Skjermingsverdige informasjonssystemer skal godkjennes som grunnlag for tillit til at sikkerhetsnivået for systemet er forsvarlig.

Skjermingsverdige informasjonssystemer godkjennes av virksomhetene selv eller av NSM, avhengig av den risiko systemene er utsatt for. Sektormyndigheter med tilsynsansvar (der slike er utpekt)[1] kan godkjenne skjermingsverdige informasjonssystemer, forutsatt at de er gitt godkjenningsmyndighet.

Hele informasjonssystemet skal godkjennes: Tjenere, periferiutstyr og klienter, for angitt funksjon og operativt miljø og med de forutsetninger og regler som gjelder for sikker bruk. Sikkerhetsgodkjenninger gjelder i inntil 5 år eller til endringer som er vesentlige for beskyttelsen av systemet, besluttes eller oppstår.

Ved særlig behov for å ta et informasjonssystem i bruk kan det gis midlertidig brukstillatelse selv om ikke alle formelle krav til sikkerhetsgodkjenning er oppfylt. En forutsetning for slik tillatelse er at alle mangler er kompensert slik at sikkerhetsnivået for systemet er forsvarlig, og at det foreligger plan for å rette manglene. NSM kan i særlige tilfeller dispensere fra krav til midlertidig brukstillatelse.

1.1. Krav om sikkerhetsgodkjenning

Skjermingsverdig informasjonssystem kan godkjennes dersom risiko forbundet med bruk av systemet er håndtert til akseptabelt nivå, og slik at sikkerhetsnivået er forsvarlig. Sikkerhetsloven har krav om sikkerhetsgodkjenning av skjermingsverdige informasjonssystemer i:

> *§ 6-3. Godkjenning av skjermingsverdige informasjonssystemer (første ledd)*
>
> *Skjermingsverdige informasjonssystemer skal godkjennes av en godkjenningsmyndighet. Informasjonssystemer som skal behandle sikkerhetsgradert informasjon, skal godkjennes før de tas i bruk.*

Kravet om sikkerhetsgodkjenning er utdypet i virksomhetsikkerhetsforskriften

> *§ 50. Plikt til å sørge for godkjenning av skjermingsverdige informasjonssystemer*
>
> *Når en virksomhet har besluttet å utvikle et skjermingsverdig informasjonssystem, skal den informere Nasjonal sikkerhetsmyndighet. Informasjonsplikten gjelder ikke dersom det ut fra § 51 er åpenbart at Nasjonal sikkerhetsmyndighet ikke trenger å godkjenne systemet.*

[1] Utpekt iht. bestemmelsene i sikkerhetsloven § 3-1, andre ledd

En virksomhet skal sørge for at informasjonssystemer som skal behandle sikkerhetsgradert informasjon, er godkjent før det de tas i bruk. Andre skjermingsverdige informasjonssystemer skal godkjennes så snart det er praktisk mulig. Virksomheten skal dekke kostnadene med godkjenningen.

Informasjonssystemer som skal behandle sikkerhetsgradert informasjon må være sikkerhetsgodkjent før det tas i bruk. Andre skjermingsverdige informasjonssystemer skal godkjennes når det er praktisk mulig. Dette må forstås slik at disse systemene skal godkjennes så snart forutsetninger og regler for sikker bruk er fastlagt og kan meddeles de som berøres, inkludert godkjenningsmyndigheten.

Det er virksomheten som beslutter å ta et skjermingsverdig informasjonssystem i bruk som har plikt til å sørge for sikkerhetsgodkjenning. Dette gjelder selv om eierskap, utvikling, driftsansvar mv. er lagt til annen virksomhet. Dersom flere virksomheter skal bruke systemet kan godkjenningen forvaltes av én av dem. Denne virksomheten må da forplikte de øvrige til de forutsetninger og regler som gjelder for sikker bruk av systemet.

Ved beslutning om å utvikle et informasjonssystem som skal godkjennes av NSM, skal NSM informeres. NSM har da behov for opplysninger om:

- overordnet beskrivelse av informasjonssystemet som inkluderer beskrivelse av systemets funksjon og operative miljø
- sikkerhetsgradering for informasjon som skal behandles i systemet eller klassifisering av objekt eller infrastruktur som systemet understøtter
- hvilke av punktene i virksomhetsikkerhetsforskriften § 51 første og andre ledd som utløser plikt til godkjenning hos NSM

Virksomheten skal dekke kostnadene ved sikkerhetsgodkjenning.

1.2. Skjermingsverdige informasjonssystemer

Sikkerhetsloven angir hvilke informasjonssystemer som er skjermingsverdige i:

§ 6-1. Skjermingsverdige informasjonssystemer (første ledd)

Et informasjonssystem er skjermingsverdig dersom det behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner.

Et skjermingsverdig informasjonssystem er et system for innsamling, registrering, sammenstilling lagring og utlevering av skjermingsverdig informasjon og/eller et system som har avgjørende betydning for en grunnleggende nasjonale funksjon.

Skjermingsverdig informasjon er informasjon som kan skade nasjonale sikkerhetsinteresser dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, jf. sikkerhetsloven § 5-1. Skjermingsverdig informasjon er følgelig informasjon som må sikres av hensyn til konfidensialitet, tilgjengelighet eller integritet.

Eksempler på skjermingsverdige informasjonssystemer er systemer for saksbehandling av sikkerhetsgradert informasjon, systemer for informasjonsbehandling i våpensystemer og prosesstyringssystemer som i seg selv er, eller som har avgjørende betydning for grunnleggende nasjonale funksjoner.

Kravet om sikkerhetsgodkjenning i sikkerhetsloven § 6-3 gjelder for hele informasjonssystemet. Det innebærer at sikkerhetsgodkjenningen normalt skal omfatte alle de deler av informasjonssystemet (tjenere, periferiutstyr og klienter) som er nødvendig for å oppnå systemets formål. Sikkerhetsgodkjenningen gjelder for den funksjon og det operative miljø som er angitt, og med de forutsetninger og regler for sikker bruk som gjelder for systemet.

En sikkerhetsgodkjenning vil gjelde for fysiske plasseringer av informasjonssystemet. Godkjenninger kan også gjelde for typiske plasseringer (for eksempel serverrom, kontorer, kjøretøy og fartøy) beskrevet gjennom forutsetningene og reglene for sikker bruk.

Virksomheten må ha oversikter over informasjonssystemets fysiske plasseringer. Informasjon om skjermingsverdige informasjonssystemer, herunder om fysiske plasseringer av slike skal være tilgjengelig for tilsynsmyndigheten, jf. sikkerhetsloven § 3-4, første ledd.

1.3. Sikkerhetsgodkjenning ved sammenkobling

Ved sammenkobling av informasjonssystemer gjelder egne bestemmelser i virksomhetsikkerhetsforskriften:

> *§ 55. Sammenkobling av informasjonssystemer som behandler sikkerhetsgradert informasjon*
>
> *Dersom en sammenkobling av flere informasjonssystemer som behandler informasjon gradert KONFIDENSIELT eller høyere, medfører at systemene sikkerhetsmessig blir avhengige av hverandre på en uoversiktlig måte, skal sammenkoblingen skje via et eget informasjonssystem.*
>
> *Slike sammenkoblinger skal reguleres i avtaler mellom de aktuelle virksomhetene. Avtalene skal avklare roller og ansvaret for sammenkoblingen og hvilken informasjon og hvilke tjenester som skal utveksles.*

Sammenkobling av skjermingsverdige informasjonssystemer godkjennes ikke separat. Slike sammenkoblinger skal være del av sikkerhetsgodkjenningen for de aktuelle systemene, det vil si at sammenkoblinger er del av funksjon og operativt miljø og påvirker beskyttelsesbehovet. Dette innebærer at hvert av de sammenkoblede systemene må ha tilstrekkelig egenbeskyttelse for å håndtere de (trussel-)scenarier som følger av sammenkoblingen.

Dersom informasjonssystemer som allerede er sikkerhetsgodkjent sammenkobles på et senere tidspunkt, er det mulig at forutsetningene for de opprinnelige godkjenningene ikke lenger er til stede. Systemene må da ha ny godkjenning.

Dersom det ved sammenkobling av informasjonssystemer for behandling av informasjon sikkerhetsgradert KONFIDENSIELT eller høyere ikke er mulig å fastlegge tydelige forutsetninger og

regler for sikker bruk, skal sammenkobling skje i eget informasjonssystem med egen sikkerhetsgodkjenning.

Virksomhetene som bruker systemet skal forplikte seg til forutsetninger og regler for sikker bruk, i en sammenkoblingsavtale. Det er ikke formkrav til sammenkoblingsavtale, men punktene under angir forhold som normalt vil omfattes av en slik avtale:

Sammenkoblingsavtale

1 Partene

2 Sammenkobling

2.1 System for sammenkobling (systembeskrivelse, sikkerhetsgodkjenning)

2.2 Systemer som sammenkobles (systembeskrivelse, sikkerhetsgodkjenning)

2.3 Beskrivelse av sammenkobling

2.4 Beskrivelse av informasjonsutveksling

3 Forutsetninger og regler for sikker bruk (med henvisning til forutsetninger og regler)

4 Håndtering av uønskede hendelser

5.1 Varsling

5.2 Strakstiltak og permanente tiltak

5 Fordeling av ansvar (system for sammenkobling)

5.1 Ansvar for sikkerhetsgodkjenninger

5.2 Ansvar for utarbeidelse, vedlikehold og fordeling av forutsetninger og regler for sikker bruk

5.3 Ansvar for forvaltning, drift og vedlikehold i hele systemenes levetid

5.4 Ansvar for oppfølging av det forebyggende sikkerhetsarbeidet (som berører informasjonssystemene)

6 Informasjonsplikt (om forhold med betydning for sikkerhet)

7 Varighet og endringer (med forutsetning om gyldige sikkerhetsgodkjenninger)

Ved sammenkobling av/med informasjonssystemerer som skal behandle informasjon sikkerhetsgradert av fremmed stat eller internasjonal organisasjon kan det gjelde andre krav enn de som omtales her.

1.4. Godkjenningsmyndighet

Virksomhetsikkerhetsforskriften fordeler godkjenningsmyndighet i:

§ 51. Godkjenningsmyndighet

Nasjonal sikkerhetsmyndighet godkjenner skjermingsverdige informasjonssystemer som er utpekt som, eller har avgjørende betydning for funksjonen til, et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK.

Nasjonal sikkerhetsmyndighet godkjenner informasjonssystemer som behandler sikkerhetsgradert informasjon og som

a) skal brukes i utlandet

b) har forbindelse til informasjonssystemer i utlandet eller til andre virksomheters informasjonssystemer

c) brukes eller har forbindelser utenfor områder virksomheten kontrollerer

d) har brukere som ikke er sikkerhetsklarert for det graderingsnivået som behandles i informasjonssystemet eller informasjonssystemer dette har forbindelse til

e) behandler informasjon som er gradert HEMMELIG, og som har brukere som ikke skal ha tilgang til all informasjon i informasjonssystemet eller de informasjonssystemer dette har forbindelse til

f) behandler informasjon som er gradert STRENGT HEMMELIG.

En virksomhet som råder over et skjermingsverdig informasjonssystem som ikke er nevnt i første eller andre ledd, skal selv godkjenne systemet. Nasjonal sikkerhetsmyndighet og relevante tilsynsmyndigheter skal informeres om slike informasjonssystemer.

Nasjonal sikkerhetsmyndighet kan bestemme at en myndighet med tilsynsansvar eller virksomheten selv skal godkjenne et informasjonssystem som nevnt i andre ledd.

Departementet som har utpekt det skjermingsverdige objektet eller infrastrukturen, kan bestemme at godkjenning av skjermingsverdige informasjonssystemer etter første ledd skal gjøres av en myndighet med tilsynsansvar. Det skal gjøres en helhetsvurdering av om myndigheten har tilstrekkelig kompetanse til å godkjenne skjermingsverdige informasjonssystemer, eller kan få slik kompetanse uten uforholdsmessig store utgifter. En uttalelse fra Nasjonal sikkerhetsmyndighet skal inngå i vurderingen.

NSM er følgelig godkjenningsmyndighet for skjermingsverdige informasjonssystemer hvor ett eller flere av følgende forhold er tilstede:

	Skjermingsverdig informasjonssystemer som behandler sikkerhetsgradert informasjon og
1	brukes i utlandet
2	har forbindelse til informasjonssystem i utlandet
3	har forbindelser til andre system enn virksomhetens informasjonssystemer
4	brukes utenfor områder virksomheten kontrollerer
5	har forbindelser utenfor områder virksomheten kontrollerer (krypterte eller ukrypterte forbindelser)

6	har brukere som ikke er sikkerhetsklarert for det graderingsnivået som behandles i informasjonssystemet
7	har brukere som ikke er sikkerhetsklarert for det graderingsnivået som behandles i informasjonssystemer det er koblet sammen med
8	behandler HEMMELIG informasjon og har brukere som ikke skal ha tilgang til all informasjon i informasjonssystemet
9	behandler HEMMELIG informasjon og har brukere som ikke skal ha tilgang til all informasjon i informasjonssystemer det er koblet sammen med
10	behandler STRENGT HEMMELIG informasjon

Videre er NSM godkjenningsmyndighet for:

Skjermingsverdig informasjonssystem som er utpekt som, eller har avgjørende betydning for, objekt eller infrastruktur klassifisert som:	
11	KRITISK
12	MEGET KRITISK

Virksomheten godkjenner selv alle øvrige skjermingsverdige informasjonssystemer, inkludert informasjonssystemer som i seg selv har avgjørende betydning for objekt eller infrastruktur klassifisert VIKTIG. NSM og sektormyndigheter med tilsynsansvar skal informeres om slike godkjenninger.

NSM kan bestemme at virksomhetene selv eller sektormyndighet med tilsynsansvar skal være godkjenningsmyndighet for informasjonssystem som beskrevet i ett eller flere av punktene 1 – 10 over. Sektordepartement kan bestemme at sektormyndighet med tilsynsansvar skal være godkjenningsmyndighet for informasjonssystem som beskrevet i pkt. 11 og/eller 12 over.

NSM og sektormyndighet med tilsynsansvar skal informeres om slike godkjenninger. Informasjon om hvem som er godkjenningsmyndighet for hvilke skjermingsverdige informasjonssystemer er tilgjengelig fra NSM, sektordepartement og sektormyndighet med tilsynsansvar.

Sikkerhetsgodkjenning gitt av NSM eller sektormyndighet med tilsynsansvar er å anse som enkeltvedtak i henhold til forvaltningslovens bestemmelser. NSMs vedtak om sikkerhetsgodkjenning kan påklages til Justis- og beredskapsdepartementet. Vedtak om sikkerhetsgodkjenning gitt av sektormyndighet med tilsynsansvar kan påklages til sektordepartementet.

1.5. Sikkerhetsgodkjenningens varighet

Sikkerhetsgodkjenningers varighet fremgår av virksomhetsikkerhetsforskriften:

§ 53. Godkjenningens varighet

En godkjenning av et skjermingsverdig informasjonssystem kan gis for inntil fem år. Hvis det oppstår en vesentlig endring som har betydning for beskyttelsen av informasjonssystemet og informasjonen, skal informasjonssystemet godkjennes på nytt.

En sikkerhetsgodkjenning er gyldig i inntil 5 år eller til det besluttes eller oppstår endringer som er vesentlige nok til at sikkerhetsnivået for informasjonssystemet ikke lenger er forsvarlig. Dette kan være

endringer i verdiene informasjonssystemet behandler eller har betydning for, endringer i systemets funksjon eller operative miljø eller ny risiko som følge av endringer i trusler eller sårbarheter.

Eksempel på endringer som nødvendiggjør ny sikkerhetsgodkjenning:

Endringer i funksjon

Virksomheten ønsker å ta i bruk videokonferansefunksjonalitet i allerede eksisterende informasjonssystem.

Endringer i operativt miljø

Et informasjonssystem som har vært godkjent for bruk i Norge skal tas i bruk i utlandet.

Nye (trussel-)scenarier

Endringer i trusler eller sårbarheter eksempelvis som følge av teknologiutvikling.

1.6. Midlertidig brukstillatelse

Krav som må oppfylles for å oppnå midlertidig brukstillatelse fremgår av virksomhetsikkerhetsforskriften:

§ 54. Midlertidig brukstillatelse

Foreligger det et særlig behov for å ta i bruk et skjermingsverdig informasjonssystem før det er godkjent, kan godkjenningsmyndigheten gi midlertidig brukstillatelse dersom

a) behovet for beskyttelse er identifisert, basert på informasjonssystemets funksjon og operative miljø

b) mangler som er forbundet med fastlegging av sikkerhetskrav, etablering av sikkerhetstiltak og sikkerhetstiltakenes funksjon, er identifisert og håndtert med kompenserende tiltak

c) det foreligger en plan for å rette manglene.

Nasjonal sikkerhetsmyndighet kan i særlige tilfeller dispensere fra kravene i første ledd.

Ved særlig behov for å ta et skjermingsverdig informasjonssystem i bruk kan det gis midlertidig brukstillatelse selv om ikke alle formelle krav til sikkerhetsgodkjenning er oppfylt, forutsatt at:

1	beskyttelsesbehovet er kjent
2	fremgangsmåte for å oppfylle beskyttelsesbehovet er fastlagt gjennom sikkerhetskrav og valg av sikkerhetstiltak
3	kompenserende tiltak er etablert der tiltak mangler slik at forsvarlig sikkerhetsnivå oppnås
4	det foreligger en plan for å rette manglene

I tillegg til dokumentasjon for godkjenning skal underlaget for midlertidig brukstillatelse omfatte informasjon om det særlige behovet og punktene 1-4 over. For å oppfylle kravene til midlertidig brukstillatelse må søknaden beskrive hvilke mangler som gjenstår i henhold til kravene i § 52.

NSM kan i særlige tilfeller dispensere fra pkt. 1 – 4 over. Det vil være et særlig tilfelle at samfunnsmessige konsekvenser ved at systemet ikke tas i bruk, overstiger konsekvensene av uønskede hendelser sammenholdt med sannsynligheten for slike hendelser.

Midlertidig brukstillatelse gitt av NSM og sektormyndighet med tilsynsansvar er å regne som enkeltvedtak i henhold til forvaltningslovens bestemmelser og kan påklages som for vedtak om sikkerhetsgodkjenning. Dispensasjoner anses også som enkeltvedtak og kan påklages.

1.7. Fakturering

NSM viser til virksomhetsikkerhetsforskriften §50 andre ledd «*Virksomheten skal dekke kostnadene med godkjenningen*». I saker hvor NSM er godkjenningsansvarlig for informasjonssystemet, vil vedtak faktureres etter følgende fastsatte gebyrsatser:

Enkel: 55 000,-	(Avslag: 27 500,-)
Middels: 165 000,-	(Avslag: 82 500,-)
Omfattende: 330 000,-	(Avslag: 165 000,-)

Gebyr settes etter en vurdering av tidsbruk, sakskompleksitet og eventuelle kostnader knyttet til rådgiving og reisevirksomhet i forkant av godkjenningsvedtaket. Gebyret settes uavhengig av vedtakstype (godkjenning, midlertidig brukstillatelse eller dispensasjon) og vedtakets varighet. Avslag faktureres 50% av gjeldende gebyrsats.

På bakgrunn av budsjettfullmakt (i Revidert Nasjonal Budsjett 2021) fra Forsvarsdepartementet (FD) vil alle vedtak om godkjenninger i forsvarssektoren belastes egen post.

NSM gjør oppmerksom på at gebyrsatsene er justert for å dekke selvkost. Faktura merkes normalt med avsenders saksreferanse og kontaktperson, samt eventuelt andre fakturaopplysninger det spesifikt er forespurt om i søknad, med forbehold om at opplysningene er ugradert.

Fakturavedtaket anses som et enkeltvedtak etter Forvaltningsloven §2

2. Grunnlag for sikkerhetsgodkjenning

Sikkerhetsgodkjenning er en planlagt og systematisk gjennomgang for å skape tillit til at sikkerhetsnivået for et informasjonssystem er forsvarlig.

Sikkerhetsgodkjenning omfatter undersøkelser av hvorvidt og hvordan risiko for uønskede hendelser er vurdert og håndtert til akseptabelt nivå. Undersøkelsene omfatter informasjonssystemets funksjon og operative miljø, beskyttelsesbehovet, krav om sikkerhetstiltak for å oppnå dette behovet og kontrollen av tiltakene.

Sikkerhetstiltak kan velges med utgangspunkt i kriterier og tiltak angitt i NSMs veiledninger som er relevante for det aktuelle informasjonssystemet. Alternativt kan tiltak velges med utgangspunkt i vurdering av sikkerhetsnivået for systemet.

Sikkerhetstiltak skal kontrolleres for å bekrefte og dokumentere at de gir akseptabel risiko og forsvarlig sikkerhetsnivå som resultat. Sikkerhetstiltak som er avgjørende for å hindre særlig kritiske uønskede hendelser skal evalueres.

2.1. Krav om forsvarlig sikkerhetsnivå

Sikkerhetsloven har krav om beskyttelse av skjermingsverdige informasjonssystemer i:

§ 6-2. Beskyttelse av skjermingsverdige informasjonssystemer (første ledd)

Virksomheten skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer, slik at

a) informasjonssystemene fungerer slik de skal

b) uvedkommende ikke får tilgang til informasjonen som behandles i systemene

c) informasjonen som behandles i systemene, ikke endres eller går tapt

d) informasjonen som behandles i systemene, er tilgjengelig ved tjenstlig behov for tilgang.

Kravet om beskyttelse er konkretisert gjennom krav til forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer i virksomhetsikkerhetsforskriften:

§ 49. Forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer

Når en virksomhet håndterer en risiko knyttet til skjermingsverdige informasjonssystemer etter § 13, skal den oppnå et forsvarlig sikkerhetsnivå ved å

a) beskytte data mot uønsket lesing og beskytte tjenester mot uønsket bruk

b) beskytte data mot uønsket modifikasjon og beskytte tjenester mot uønsket modifikasjon og manipulasjon

c) beskytte data mot uønsket sletting og beskytte tjenester mot uønsket reduksjon eller stans

d) indentifisere og autentisere brukere som kan påvirke informasjonssystemets funksjon, eller som kan få tilgang til data i systemet, før de gis tilgang til data og tjenester

e) forhindre at falske data og tjenester introduseres i informasjonssystemet

f) registrere bruk, misbruk og forsøk på misbruk av informasjonssystemet, tjenester og data

g) systematisk kontrollere at sikkerhetstiltakene er korrekt implementert og ivaretar sikkerheten på en effektiv og hensiktsmessig måte.

Sikkerhetstiltak skal være tilpasset systemets totale omfang og kompleksitet gjennom hele systemets levetid.

Sikkerhetstiltak som skal virke hurtig, eller som lett kan utløse feil når de utføres manuelt, skal automatiseres så langt det er praktisk mulig.

Virksomheten skal sørge for forsvarlig sikkerhetsnivå for skjermingsverdig informasjonssystem gjennom nødvendig beskyttelse av systemets funksjon, og av konfidensialitet, integritet og tilgjengelighet for informasjon som behandles i systemet. Forsvarlig sikkerhetsnivå oppnås ved å redusere risiko for uønskede hendelser til akseptabelt nivå.

Sikkerhetstiltak etableres i henhold til prinsippene angitt i virksomhetsikkerhetsforskriften § 15, og for å oppnå beskyttelse som beskrevet i punktene a) – g) i virksomhetsikkerhetsforskriften § 49 første ledd.

Sikkerhetstiltak kan etableres som hensiktsmessige balanserte kombinasjoner av fysiske, tekniske, organisatoriske og menneskelige tiltak. Tiltakene skal gi forsvarlig sikkerhetsnivå for hele systemet i hele levetiden. Tiltakene skal, når det er nødvendig for å oppnå akseptabel risiko og praktisk mulig, virke automatisk.

2.2. Krav til sikkerhetsgodkjenning

Virksomhetsikkerhetsforskriften har krav til hva godkjenning av skjermingsverdige informasjonssystemer innebærer og skal omfatte, i:

§ 52. Godkjenning av et skjermingsverdig informasjonssystem

Godkjenningen av et skjermingsverdig informasjonssystem er en planlagt og systematisk gjennomgang av om virksomheten har oppnådd et forsvarlig sikkerhetsnivå. Virksomheten skal dokumentere at den på en tilfredsstillende måte har vurdert og håndtert risikoen, og den skal i forbindelse med dette ha

a) identifisert behovet for beskyttelse, basert på informasjonssystemets funksjon og operative miljø

b) fastsatt sikkerhetskrav ut fra behovet for beskyttelse

c) etablert sikkerhetstiltak som oppfyller sikkerhetskravene gjennom hele informasjonssystemets levetid

d) kontrollert at sikkerhetstiltakene fungerer etter sin hensikt.

Sikkerhetsgodkjenning skal gjennomføres planlagt og systematisk iht. prosedyrer fastlagt på forhånd. Kravet gjelder uavhengig av om NSM, virksomheten selv eller sektormyndighet med tilsynsansvar er godkjenningsmyndighet.

Sikkerhetsgodkjenninger skal gjennomføres med uavhengighet tilsvarende som beskrevet i virksomhetsikkerhetsforskriften § 6 om skille mellom kontrollerende og utøvende oppgaver. Dette innebærer at ansvar for sikkerhetsgodkjenning bør legges til andre enn de som har utviklet og drifter informasjonssystemet, og at ansvar for kontroll av sikkerhetstiltak bør legges til andre enn de som har valgt eller etablert tiltakene.

Sikkerhetsgodkjenning gjennomføres ved hjelp av undersøkelser av hvorvidt og hvordan risiko for uønskede hendelser er vurdert og håndtert til akseptabelt nivå. Disse undersøkelsene omfatter funksjon og operativt miljø, beskyttelsesbehov, krav (til sikkerhetstiltak) og kontroll av disse tiltakene.

2.2.1. Funksjon og operativt miljø (systembeskrivelse)

Informasjonssystemets funksjon angis ved informasjon om systemets formål og den behandling som skal gjennomføres eller de funksjoner systemet har (avgjørende) betydning for. Informasjonen skal omfatte opplysninger om teknologi, systemets konfigurasjon og tjenester:

Beskrivelse av funksjon:

Formål

Informasjonssystemets formål – knyttet til behandling av skjermingsverdig informasjon og/eller betydning for grunnleggende nasjonal funksjon.

Sikkerhetsgodkjenning/klassifisering

(Høyeste) Graderingsnivå for informasjon som behandles i informasjonssystemet og/eller klassifisering (ev. informasjon om grunnleggende funksjon informasjonssystemet har avgjørende betydning for).

Teknologi

Grunnleggende teknologisk løsning og arkitektur – operativsystem, klient/tjener-løsning.

Sammenkoblinger og forbindelser

Informasjon om sammenkobling og dataoverføring, herunder om:

- sammenkobling med andre informasjonssystemer, inkl. informasjon om disse systemenes sikkerhetsgodkjenninger
- dataoverføring innenfor eller utenfor kontrollert, beskyttet eller sperret sone

Konfigurasjon

Systemteknisk og fysisk utforming, periferutrusting …

Tjenester

Verktøy, applikasjoner …

Informasjonssystemets operative miljø angis gjennom informasjon om fysiske, tekniske, organisatoriske og menneskelige forhold der systemet skal brukes. Disse forholdene kan være forskjellige for forskjellige deler av informasjonssystemet og beskrivelsen må omfatte hele det operative miljøet (alle fysiske og/eller typiske plasseringer):

Beskrivelse av operativt miljø:

Fysiske forhold

Informasjon om informasjonssystemets fysiske og/eller typiske plasseringer, herunder om plasseringen helt eller delvis er:

1 i Norge, NATO/EU, eller utenfor

2 innenfor eller utenfor nasjonal kontroll

3 innenfor eller utenfor kontrollert, beskyttet eller sperret sone

Elektroniske forhold

Informasjon om teknologi en trusselaktør kan benytte for å påvirke informasjonssystemet:

4 TEMPEST-avlesning, GPS-jamming og keylogging

Menneskelige forhold

Informasjon om mennesker som kan påvirke beskyttelsen av informasjonssystemet, herunder om:

10 egne medarbeidere (og innleide) med tilgang og/eller adgang til informasjonssystemet (brukere)

11 egne medarbeidere (og innleide) med muligheter for tilgang og/eller adgangs til informasjonssystemet

12 andre (eksterne) som med mulighet for å påvirke beskyttelsen av informasjonssystemet

Organisatoriske forhold

Informasjon om organisasjonen som håndterer informasjonssystemet i virksomheten eller på virksomhetens vegne, herunder om ansvar for:

13 forvaltning, drift og vedlikehold i hele systemenes levetid

14 utarbeidelse, vedlikehold og fordeling av forutsetninger og regler for sikker bruk

15 sikkerhetsgodkjenninger

16 oppfølging av det forebyggende sikkerhetsarbeidet (som berører informasjonssystemet)

Informasjonen om funksjon og miljø benyttes som grunnlag for fastlegging av beskyttelsesbehov, og for avklaring av godkjenningsmyndighet, jf. kap. 1.4 i denne veiledningen.

2.2.2. Beskyttelsesbehov

Skjermingsverdige informasjonssystemer som behandler sikkerhetsgradert informasjon (graderte informasjonssystemer) må sikres i forhold til graderingsnivået for informasjonen som behandles.

Skjermingsverdige informasjonssystemer som behandler informasjon med annet beskyttelsesbehov enn konfidensialitet eller som i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner (skjermingsverdige ugraderte informasjonssystemer) må sikres tilsvarende deres kritikalitet for funksjonen.

Informasjonssystemsikkerhet må ses i nær sammenheng med objekt- og infrastruktursikkerhet. Det kan i flere tilfeller være aktuelt å utpeke skjermingsverdige ugradert informasjonssystemer som skjermingsverdig objekt eller infrastruktur. Det er følgelig naturlig å ta utgangspunkt i klassifiseringssystemet for objekt og infrastruktur for å fastlegge hvilken grad av sikring som er nødvendig for et ugradert skjermingsverdig informasjonssystem.

Beskyttelsesbehovet angis med utgangspunkt i de av kravene til beskyttelse i virksomhetsikkerhetsforskriften § 49 a) – g). Informasjon om beskyttelsesbehov er grunnlag for valg av de sikkerhetstiltak som er nødvendig for å håndtere risiko til akseptabelt nivå og slik oppnå forsvarlig sikkerhetsnivå.

2.2.3. Sikkerhetstiltak

Ved valg av tiltak ses det bla. hen til virksomhetsikkerhetsforskriften § 15. Prinsipper ved valg og utforming av sikkerhetstiltak, samt til kap. 4, inkludert § 22 om forsvarlig sikkerhetsnivå for skjermingsverdig informasjon.

Sikkerhetstiltak velges gjennom ett av følgende alternativer:

alternativ 1 – valg av sikkerhetstiltak med utgangspunkt i NSMs anbefalinger

Sikkerhetstiltak velges med utgangspunkt i NSMs sikkerhetsfaglige anbefalinger, eksempelvis gitt i tekniske veiledninger eller håndbøker. Det er en forutsetning at anbefalingene benyttes for forholdene de er utformet for og i samsvar med de rammer og forutsetninger som er lagt til grunn, godkjennes. Sikkerhetsgodkjenning gjennomføres da samsvarsvurdering med anbefalingene.

Det kan selvsagt benyttes andre løsninger enn de NSM anbefaler og NSM har heller ikke gitt anbefalinger for alle forhold. I så fall velges sikkerhetstiltak med utgangspunkt i:

alternativ 2 – valg av sikkerhetstiltak i forhold til risiko (sikkerhetsnivå)

Sikkerhetstiltak velges etter vurdering av tiltakenes tilstrekkelighet og hensiktsmessighet i forhold til aktuelle scenarier overfor beskyttelsesbehovet. Scenariene utrykkes som relevante uønskede hendelser det må beskyttes mot, og konkretiseres ved å angi mulige aktører bak hendelsene beskrevet ved:

tilhørighet

- *eget personell*[2] *med tilgang* – dvs. medarbeidere i arbeidsforhold og som oppfyller ev. vilkår for tilgang i form av sikkerhetsklarering, autorisasjon og tjenstlige behov
- *eget personell uten tilgang* – dvs. medarbeidere i arbeidsforhold
- *eksternt personell* – som ikke har tilknytting til virksomheten

kapasitet (eller evne)

- *liten* – grunnleggende kompetanse, kjennskap til funksjon og operativt miljø fra åpne kilder, allment tilgjengelige ressurser

[2] *eget personell* omfatter også innleide og personell hos leverandører når forhold med betydning for sikkerhet er regulert i avtale tilsvarende som for medarbeidere i arbeidsforhold

- *middels* – utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø, tilpassede ressurser
- *god* – tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø, nødvendige ressurser

intensjon (eller vilje)

- *ubevisst,* uønsket handling
- *bevisst,* opportunistisk handling
- handling *med hensikt* og plan

Sikkerhetstiltakenes tilstrekkelighet og hensiktsmessighet vurderes:

- for hver av scenariene det må beskyttes mot
- i forhold til sikkerhetsgradering for berørt informasjon/klassifisering av berørt informasjonssystem, objekt eller infrastruktur

… samt i henhold til følgende sammenstilling:

Vurdering i forhold til sikkerhetsgradering[3]

	EGET PERSONELL MED TILGANG	EGET PERSONELL UTEN TILGANG	EKSTERNE
BEGRENSET	**liten kapasitet** *eller* **ubevisst**	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**
KONFIDENSIELT	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**
HEMMELIG	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**
STRENGT HEMMELIG	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**

Leseveiledning:

BEGRENSET

Informasjonssystemet skal være sikret slik at eget personell (med eller uten tilgang) ikke kan forårsake uønskede hendelser overfor informasjonssystem som behandler informasjon sikkerhetsgradert BEGRENSET når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

[3] Skjermingsverdig informasjon som ikke er sikkerhetsgradert, det vil si som må beskyttes av andre hensyn en konfidensialitet, vurderes i forhold til klassifiseringen for informasjonssystem, objekt eller infrastruktur som berøres dersom informasjonen går tapt, blir endret eller blir utilgjengelig.

Eksterne skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

KONFIDENSIELT

Informasjonssystemet skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser overfor informasjonssystem som behandler informasjon sikkerhetsgradert KONFIDENSIELT når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eget personell (uten tilgang) skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

Eksterne skal ikke kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

HEMMELIG

Informasjonssystemet skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser overfor informasjonssystem som behandler informasjon sikkerhetsgradert HEMMELIG selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser– ved bevisst opportunistisk handling.

Verken eget personell (uten tilgang) eller eksterne skal kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan..

STRENGT HEMMELIG

Det skal ikke være mulig å forårsake uønskede hendelser overfor informasjonssystem som behandler informasjon sikkerhetsgradert STRENGT HEMMELIG selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – og selv om det foreligger hensikt og plan.

Eksempler på vurdering av sikkerhetstiltak:

BEGRENSET

Situasjon: Skriver er tilkoblet informasjonssystem for behandling av informasjon sikkerhetsgradert BEGRENSET og er plassert i område der både medarbeidere med og uten tilgang til informasjon sikkerhetsgradert BEGRENSET, har adgang. Dokumenter skrives ut straks de sendes til utskrift. Virksomhetens sikkerhetsinstruks har ikke regler om håndtering av utskrifter.

Scenario: Medarbeidere (med eller uten tilgang) tar ved feil med seg (deler av) andres utskrifter med sikkerhetsgradert informasjon, og sender disse ut av virksomheten.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at *egne medarbeidere (med eller uten tilgang)*, ubevisst kan kompromittere informasjon sikkerhetsgradert BEGRENSET. Sikkerhetsnivået er følgelig ikke forsvarlig.

KONFIDENSIELT

Situasjon: Innleid renholdspersonell har tilgang til kontorlandskap etablert som beskyttet sone. Informasjonssystem for behandling av informasjon sikkerhetsgradert KONFIDESIELT er plassert i sonen. Det er ikke etablert automatisk skjermsparer for, eller låsing av, informasjonssystemets arbeidsstasjoner. Virksomhetens sikkerhetsinstruks har ikke regler for bruk av skjermsparer eller regler for låsing.

Scenario: Innleid renholdspersonell blir fulgt av personell med permanent adgang til den beskyttede sonen, men får ved gjennomføring av renholdet likevel innsyn i informasjon på arbeidsstasjonenes skjermer.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at *egne medarbeidere uten tilgang* (innleid rengjøringspersonell), bevisst og opportunistisk kan tilegne seg informasjon sikkerhetsgradert KONFIDENSIELT. Sikkerhetsnivået er følgelig ikke forsvarlig.

HEMMELIG

Situasjon: En virksomhet er lokalisert i et forretningsbygg med flere andre eksterne virksomheter i tilstøtende lokaler. Virksomheten har ikke oversikt over hvem som har tilgang til de tilstøtende lokalene.

Virksomheten behandler sikkerhetsgradert informasjon HEMMELIG, men har ikke sikrede rom eller lokaler for tale sikkerhetsgradert HEMMELIG. Når virksomheten behandler og diskuterer informasjon sikkerhetsgradert HEMMELIG gjøres dette på dedikert kontor. Sikkerhetsinstruksen har regler som beskriver at alt av elektronisk utstyr ikke skal medbringes inn i rommet.

Scenario: Statlig trusselaktør har lokaler i etasje umiddelbart over virksomheten og kan via tekniske hjelpemidler få tilgang til informasjon som behandles i etasjen under.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at *eksterne* med hensikt, plan og tilpasset kompetanse kan kompromittere informasjon sikkerhetsgradert HEMMELIG. Sikkerhetsnivået er følgelig ikke forsvarlig.

STRENGT HEMMELIG

Situasjon: Informasjonssystem for behandling av informasjon sikkerhetsgradert STRENGT HEMMELIG er plassert i sperret område og for bruk av en (autorisert og sikkerhetsklarert) medarbeider av gangen. Systemet har ingen eksterne tilkoblinger eller flyttbare lagringsmedier, men mulighet for kopiering av sikkerhetsgradert informasjon til flyttbart lagringsmedium.

Scenario: Egne medarbeidere med tilgang til det aktuelle informasjonssystemet kan kopiere sikkerhetsgradert informasjon til medbrakt flyttbart lagringsmedia og ta informasjonen med ut av virksomheten.

Vurdering: Gjeldende sikkerhetsnivå muliggjøre at egne *medarbeidere med tilgang* med hensikt og plan og tilpasset kompetanse kan kompromittere informasjon sikkerhetsgradert STRENGT HEMMELIG. Sikkerhetsnivået er følgelig ikke forsvarlig.

Vurdering i forhold til klassifisering[4]

	EGET PERSONELL MED TILGANG	EGET PERSONELL UTEN TILGANG	EKSTERNE
UNDERSTØTTER	**liten kapasitet** *eller* **ubevisst**	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**

[4] Sammenstillingen benyttes for vurdering av klassifisert objekt og infrastruktur. Den benyttes også for vurdering av informasjonssystem som ikke selv er klassifisert (som objekt) men som har avgjørende betydning for klassifisert objekt eller infrastruktur, og sammenstillingen benyttes for vurdering av skjermingsverdig informasjon som ikke er sikkerhetsgradert, det vil si som må beskyttes av andre hensyn en konfidensialitet. Vurderingen gjennomføres da i forhold til klassifiseringen for objekter eller infrastruktur som berøres dersom informasjon går tapt, blir endret eller blir utilgjengelig.

Med *understøtter* menes informasjonssystem som ikke er skjermingsverdig, det vil si som ikke har avgjørende betydning for klassifisert objekt (og heller ikke selv er klassifisert), men som likevel har betydning for slike. Sikkerhetslovens krav om forsvarlig sikkerhetsnivå skal forstås slik at også slike systemer må sikres i nødvendig grad. Det er imidlertid ikke krav om godkjenning av disse informasjonssystemene.

VIKTIG	**liten kapasitet** *eller* **ubevisst**	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**
KRITISK	**middels kapasitet** *eller* **bevisst**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**
MEGET KRITISK	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**	**stor kapasitet** *eller* **med hensikt**

Leseveiledning:

UNDERSTØTTER

Informasjonssystemet skal være sikret slik at ikke eget personell (med eller uten tilgang) kan forårsake uønskede hendelser som påvirker funksjon i informasjonssystem som UNDERSTØTTER skjermingsverdig objekt, eller infrastruktur, når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eksterne skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

VIKTIG

Informasjonssystemet skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser som påvirker funksjon i informasjonssystem med avgjørende betydning for objekt eller infrastruktur klassifisert VIKTIG når de kun har grunnleggende kompetanse, informasjon fra åpne kilder og allment tilgjengelige ressurser – ved ubevisst uønsket handling.

Eget personell (uten tilgang) skal ikke kunne forårsake slike hendelser selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

Eksterne skal ikke kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

KRITISK

Informasjonssystemet skal være sikret slik at eget personell (med tilgang) ikke kan forårsake uønskede hendelser som påvirker funksjon i informasjonssystem med avgjørende betydning for objekt eller infrastruktur klassifisert KRITISK selv med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser – ved bevisst opportunistisk handling.

Eget personell (uten tilgang) eller eksterne skal ikke kunne forårsake slike hendelser selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – selv om det foreligger hensikt og plan.

MEGET KRITISK

Det skal ikke være mulig å forårsake uønskede hendelser overfor informasjonssystem med avgjørende betydning for objekt eller infrastruktur klassifisert MEGET KRITISK selv med tilpasset kompetanse, inngående kjennskap til funksjon og operativt miljø og nødvendige ressurser – og selv om det foreligger hensikt og plan.

Eksempler på vurdering av sikkerhetstiltak:

UNDERSTØTTER

Situasjon: Virksomheten har medarbeidere med tilganger til informasjonssystem som understøtter skjermingsverdig verdi. Virksomheten har ikke regler for oppdatering av tilgangsstyring og påloggingsrutiner, når ansatte slutter.

Scenario: Tidligere ansatte (eksterne) benytter gammel påloggingsdata og kjennskap til virksomhetens rutiner for å få tilgang til informasjonssystemet, og kan med dette forårsake uønskede hendelser overfor den skjermingsverdige verdien.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at *eksterne* med utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser, bevisst kan påvirke funksjonen i informasjonssystem som understøtter skjermingsverdig verdi. Sikkerhetsnivået er følgelig ikke forsvarlig.

VIKTIG

Situasjon: Tjener i informasjonssystem med avgjørende betydning for skjermingsverdig verdi klassifisert VIKTIG er plassert i felles serverrom der også driftspersonell uten tjenstlig behov for tilgang til den aktuelle tjeneren (kun med behov for tilgang til annet utstyr) har adgang.

Scenario: Medarbeidere uten tilgang til det aktuelle informasjonssystemet kan gjennom adgang til serverrommet forårsake driftsavbrudd for tjeneren i informasjonssystemet.

Vurdering: Gjeldende sikkerhetsnivå muliggjøre at *egne medarbeidere uten tilgang* og som (gjennom sin stilling) har utvidet kompetanse, kjennskap til intern informasjon om funksjon og operativt miljø og tilpassede ressurser, bevisst kan påvirke funksjonen i informasjonssystem med avgjørende betydning for skjermingsverdig verdi klassifisert VIKTIG. Sikkerhetsnivået er følgelig ikke forsvarlig.

KRITISK

Situasjon: Medarbeidere med tilgang til informasjonssystem med avgjørende betydning for skjermingsverdig verdi klassifisert KRITISK har rettigheter for bruk av systemet utover tjenstlig behov.

Scenario: Medarbeidere med tilgang til det aktuelle informasjonssystemet kan benytte utvidede rettigheter for bruk av systemet til uønsket modifikasjon av data og til å hindre registrering av bruk av systemet.

Vurdering: Gjeldende sikkerhetsnivå muliggjør at *egne medarbeidere med tilgang* og med tilpassede ressurser (gjennom utvidede rettigheter), bevisst kan påvirke funksjonen i informasjonssystem avgjørende betydning for skjermingsverdig verdi klassifisert KRITISK. Sikkerhetsnivået er følgelig ikke forsvarlig.

MEGET KRITISK

Situasjon: Datasenter klassifisert som MEGET KRITISK skjermingsverdig verdi er plassert i et eget avlåst lokale i en fjellhall. Fjellhallen eies og driftes av en privat virksomhet. Denne har ansvar for vakthold, drift og leveranse av felles kjøle- og strømanlegg. Også andre virksomheter leier lokaler i fjellhallen. Alle leietakerne har tilgang til kjøle- og strømanleggene.

Scenario: Medarbeidere hos andre virksomheter har tilgang til og kan forårsake svikt i kjøle- eller strømanleggene

Vurdering: Gjeldende sikkerhetsnivå muliggjør at *eksterne* med tilpasset kompetanse, nødvendige ressurser og med hensikt og plan vil kunne forårsake uønskede hendelser overfor skjermingsverdig verdi klassifisert MEGET KRITISK. Sikkerhetsnivået er følgelig ikke forsvarlig.

2.2.4. Kontroll av sikkerhetstiltak

Virksomheten skal kontrollere at sikkerhetstiltak er etablert og fungerer etter hensikten, dvs. at risiko for uønskede hendelser reduseres til akseptabelt nivå slik at forsvarlig sikkerhetsnivå er oppnådd for informasjonssystemet. Dersom kontrollen avdekker at forsvarlig sikkerhetsnivå ikke er oppnådd, må tiltakene endres eller erstattes og ny kontroll gjennomføres.

Kontroller kan gjennomføres som (tekniske) undersøkelser, (IKT-)sikkerhetsrevisjoner eller dokumentgjennomganger, og kan omfatte automatiserte undersøkelse av eksempelvis funksjoner og sårbarheter.

Alle sikkerhetstiltak skal kontrolleres, men dersom et tiltak ivaretas av flere komponenter som utfører identiske oppgaver, er det tilstrekkelig å teste et utvalg av disse. Dette kan eksempelvis gjelde identiske dioder, sensorer, brannmurer eller switcher som er konfigurert likt på ulike installasjonssteder.

Det stilles ikke formkrav til dokumentering av kontroller, men dokumentasjonen må som minimum angi sammenhengen mellom beskyttelsesbehov og tiltak sammen med kontrollresultatene for det enkelte tiltak.

2.3. Evaluering av produkter og tjenester

Virksomhetsikkerhetsforskriften har krav om evaluering av produkter og tjenester i:

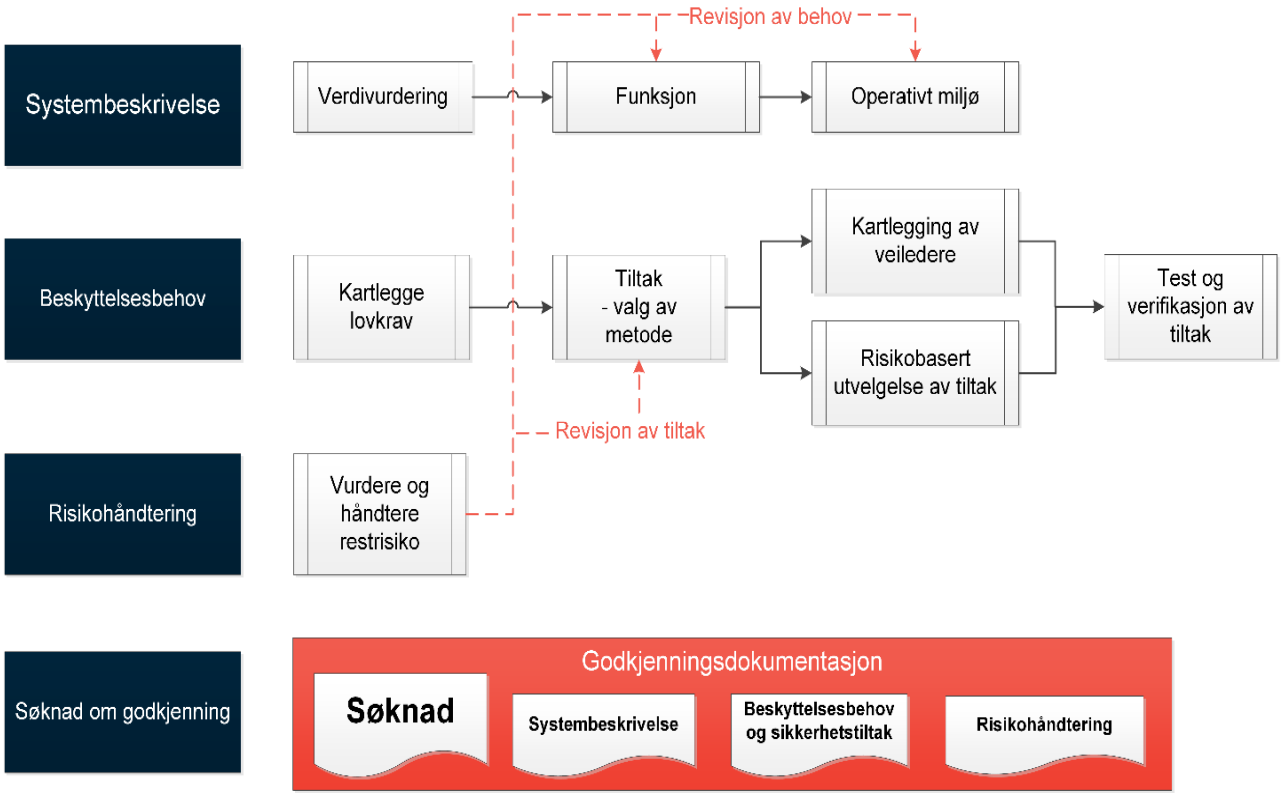
> *§ 16. Krav om bruk av evaluerte produkter og tjenester*
>
> *Når en virksomhet velger sikkerhetstiltak, skal den bruke evaluerte produkter og tjenester dersom produktets eller tjenestens funksjon i seg selv er avgjørende for at*
>
> *a) personer ikke får tilgang til informasjon gradert HEMMELIG eller STRENGT HEMMELIG uten å ha et tjenstlig behov for det*
>
> *b) personer ikke får tilgang til sikkerhetsgradert informasjon de ikke er autorisert for*
>
> *c) personer ikke kan overta eller sette ut av drift infrastruktur eller objekter som er klassifisert KRITISK eller MEGET KRITISK.*
>
> *Evalueringen skal skje gjennom metodisk utvikling og testing av produktet eller tjenesten og være etterprøvbar. Den skal utføres av Nasjonal sikkerhetsmyndighet eller et akkreditert laboratorium utpekt av Nasjonal sikkerhetsmyndighet, gi tillit til produktet eller tjenesten og sikre at produktet eller tjenesten har nødvendig funksjonalitet for å sikre det aktuelle graderingsnivået eller klassifiseringsnivået. Nasjonal sikkerhetsmyndighet kan godkjenne bruk av produkter og tjenester som er evaluert eller sertifisert i andre land.*

Sikkerhetstiltak som er avgjørende eller eneste beskyttelse for tilfeller som omfattes av bokstav a til c i virksomhetsikkerhetsforskriften § 16 skal kontrolleres ved hjelp av evaluering av de produkter og tjenester tiltaket består av. Dette innebærer blant annet at det ikke er krav om evaluering når det er redundans i sikkerhetstiltakene

Evaluering er metodisk og etterprøvbart gjennomgang og prøving av produkter eller tjenester utført av NSM eller akkreditert prøvingslaboratorium utpekt av NSM. Evaluering kan dokumenteres gjennom sertifisering. NSM kan godkjenne bruk av produkter og tjenester evaluert eller sertifisert i andre land.

Informasjon om evaluerte produkter og tjenester, og om avtaler om aksept av evalueringer og sertifiseringer utført i andre land er tilgjengelig hos NSM.

Vedlegg 1 – Sikkerhetsgodkjenning som en del av utviklingsprosess



Vedlegg 2 – Eksempler på underlag for sikkerhetsgodkjenning

Det følgende er eksempler på beskrivelse for sikkerhetsgodkjenning av et skjermingsverdig informasjonssystem med begrenset kompleksitet. Beskrivelser av mer komplekse informasjonssystemer må inneholde samme typer opplysninger men vil nødvendigvis være mer omfattende.

Systembeskrivelse for <informasjonssystem>

1 Funksjon

1.1 Formål

Informasjonssystemet benyttes for registrering og oppbevaring av trusselvurderinger.

1.2 Sikkerhetsgradering

Høyeste sikkerhetsgradering for informasjon som behandles i informasjonssystemet er STRENGT HEMMELIG

1.3 Teknologi

Informasjonssystemet består av en frittstående PC med operativsystem Microsoft Windows 10 pro.

1.4 Konfigurasjon

Informasjonssystemet består av stasjonær PC med skjerm, tastatur og mus. Systemet har ingen perifere enheter og ingen (muligheter for) datakommunikasjon.

1.5 Tjenester

Informasjonssystemet har verktøy for tekstbehandling (Microsoft Word 2010), tekstlesing (Adobe Acrobat Reader XI) og applikasjon for arkivering av dokumenter.

2 Operativt miljø

2.1 Fysiske forhold

Informasjonssystemet er plassert i Norge, innenfor nasjonal kontroll og i sperret sone.

2.2 Elektroniske forhold

Informasjonssystemet er ikke koblet sammen med andre informasjonssystemer. Det er ingen dataoverføring til/fra informasjonssystemet.

2.3 Menneskelige forhold

5 medarbeidere i <Avdeling> har tilgang og adgang til informasjonssystemet i tillegg har Sikkerhetsleder i <Virksomhet> nødvendig tilgang og adgang for oppfølging av sikkerhetsarbeid.

Ingen andre medarbeidere, innleide eller eksterne har mulighet for tilgang eller adgang til informasjonssystemet.

2.4 Organisatoriske forhold

Informasjonssystemet benyttes utelukkende av <Avdeling>

Avdelingsleder i <Avdeling> er ansvarlig for forvaltning, drift og vedlikehold av informasjonssystemet i hele levetiden.

Avdelingsleder i <Avdeling> er ansvarlig for utarbeidelse, vedlikehold og fordeling av forutsetninger og regler for sikker bruk.

Datasikkerhetsleder i <Virksomhet> påser at informasjonssystemets sikkerhetsgodkjenning herunder om endringer gir behov for regodkjenning.

Sikkerhetsleder i <Virksomhet> er ansvarlig for oppfølging av det forbyggende sikkerhetsarbeidet, herunder den delen av arbeidet som berører informasjonssystemet.

Beskyttelsesbehov og sikkerhetstiltak for <Informasjonssystem>

1 Beskyttelsesbehov

1.1 Data i informasjonssystemet må beskyttes mot uønsket lesning og informasjonssystemets tjenester skal beskyttes mot uønsket bruk.

1.2 Data i informasjonssystemet må beskyttes mot uønsket modifikasjon og informasjonssystemets tjenester må beskyttes mot uønsket modifikasjon og manipulasjon.

1.3 Data i informasjonssystemet må beskyttes mot uønsket sletting og informasjonssystemets tjenester må beskyttes mot uønsket reduksjon.

1.4 Brukere må identifiseres og autentiseres før de får tilgang til informasjonssystemet.

1.5 Introduksjon av falske data og tjenester i informasjonssystemet, må forhindres.

1.6 Bruk, misbruk og forsøk på misbruk av informasjonssystemet, tjenester og data må registreres.

1.7 Sikkerhetstiltakenes implementering, effektivitet og hensiktsmessighet må kontrolleres systematisk.

2 Scenarier og sikkerhetstiltak

BESKYTTELSES-BEHOV	SCENARIER/HENVISNING TIL NSMS ANBEFALING	SIKKERHETSTILTAK	KONTROLL
…	…	…	…
1.1	Egne medarbeidere med tilgang til det aktuelle informasjonssystemet kan kopiere sikkerhetsgradert informasjon til medbrakt flyttbart lagringsmedia og fordele informasjonen ut av virksomheten.	…	…
		Tilgangskontroll for individuell identifisering og autentisering er etablert.	Funksjonsprøving av system for tilgangs-kontroll og undersøkelse av rutiner for tilgangskontroll
		Fysiske og systemtekniske tiltak som forhindrer tilkobling av eksterne lagringsmedier er etablert	Funksjonsprøving
		…	…

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no