

|  |
| --- |
|  |
| Søknad om godkjenning av skjermingsverdig informasjonssystem  |
|   |

|  |  |
| --- | --- |
|  |  |



Versjon: 1.0

 **Bakgrunn**

**[Klassifisering]
iht. [iht.]**

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 sine ansvarsområder vedta at andre virksomheter 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.

Skjermingsverdige informasjonssystemer skal godkjennes av en godkjenningsmyndighet. Det er virksomheten som beslutter å ta informasjonssystemet i bruk som har plikt til å sørge for godkjenning. Informasjonssystem som skal behandle sikkerhetsgradert informasjon må være godkjent før det tas i bruk. Andre skjermingsverdige informasjonssystemer skal godkjennes så snart det er praktisk mulig.

Et informasjonssystem godkjennes når risiko forbundet med bruk av systemet er håndtert til akseptabelt nivå slik at sikkerhetsnivået er forsvarlig. Risiko og sikkerhetsnivå fastslås etter vurdering av informasjonssystemets verdi, funksjon, operative miljø, beskyttelsesbehov og av sikkerhetstiltakene.

NSM skal informeres når en virksomhet har besluttet å utvikle et skjermingsverdig informasjonssystem. NSM skal også informeres når virksomheten selv godkjenner et skjermingsverdig informasjonssystem.

Virksomheten skal dekke alle kostnader forbundet med godkjenning av skjermingsverdig informasjonssystem. Informasjon om NSMs gebyrer er tilgjengelig fra NSM. NSMs *Veileder for godkjenning av informasjonssystem* gir utfyllende informasjon om godkjenning.

Dette dokumentet angir den informasjon som skal oversendes NSM ved:

* beslutning om å utvikle et skjermingsverdig informasjonssystem. I så fall benyttes *Del 1* og *2* så langt det er mulig. Ny/endret informasjon oversendes når den blir tilgjengelig.
* virksomhetens egen godkjenning av et skjermingsverdig informasjonssystem. I så fall benyttes *Del 1, 2* og *3*.
* søknad til NSM om godkjenning av skjermingsverdig informasjonssystem[[1]](#footnote-1). I så fall benyttes *Del 1, 2* og *4*. I tillegg legges nødvendige skisser/tabeller og tegninger av informasjonssystemet med infoflyt og sammenkoblinger med som vedlegg.

Informasjonen vil normalt være skjermingsverdig. Virksomheten må verdivurdere denne informasjonen, gradere informasjonen og påføre graderingsmerke. Avhengig av gradering kan informasjonen oversendes elektronisk eller ved kurer.

# Del 1 – Godkjenningsmyndighet

Virksomheten selv, sektormyndighet med tilsynsansvar eller NSM, er godkjenningsmyndighet. Informasjon om sektormyndigheter med tilsynsansvar og hvilke av disse som kan godkjenne skjermingsverdige informasjonssystemer, er tilgjengelig fra NSM.

*Pkt. 1.1* og *1.2* benyttes for å avgjøre om NSM eller virksomheten selv er godkjenningsmyndighet. Om alle spørsmålene bevares med NEI skal virksomheten godkjenne informasjonssystemet. Om ett av spørsmålene besvares med JA er NSM godkjenningsmyndighet[[2]](#footnote-2).

## For skjermingsverdig gradert informasjonssystem

Hvem som er godkjenningsmyndighet for informasjonssystem som behandler sikkerhetsgradert informasjon, avhenger av graderingen og informasjonssystemets funksjon og operative miljø.

|  |  |
| --- | --- |
| Skal informasjonssystemet brukes i utlandet? | JA / NEI |
| Har informasjonssystemet forbindelser til informasjonssystemer i utlandet eller til andre virksomheters informasjonssystemer? | JA / NEI |
| Brukes eller har informasjonssystemet forbindelser utenfor områder virksomheten kontrollerer? | JA / NEI |
| Har informasjonssystemet brukere som ikke er sikkerhetsklarert for det graderingsnivået som behandles i informasjonssystemet eller systemer dette har forbindelse til? | JA / NEI |
| Behandler systemet informasjon gradert HEMMELIG og har brukere som ikke skal ha tilgang til all informasjon i systemet, eller systemer dette har forbindelse til? | JA / NEI |
| Behandler systemet informasjon gradert STRENGT HEMMELIG? | JA / NEI |
| Skal informasjonssystemet behandle NATO-gradert informasjon? | JA / NEI |

## For skjermingsverdig ugradert informasjonssystem

Hvem som er godkjenningsmyndighet for informasjonssystem som er utpekt som, eller har avgjørende betydning for funksjonen til objekt eller infrastruktur, avhenger av klassifiseringen.

|  |  |
| --- | --- |
| Er informasjonssystemer utpekt som, eller har avgjørende betydning for funksjonen til et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK? | JA / NEI |

# Del 2 – Virksomhet og informasjonssystem

Det er virksomheten som beslutter å ta informasjonssystemet i bruk som har plikt til å sørge for godkjenning. Ev. godkjenning vil gjelde for et nærmere beskrevet informasjonssystem i nærmere angitte operative miljøer.

## Virksomhet

Virksomheten som søker godkjenning beskrives her. Dersom flere virksomheter skal bruke systemet, kan disse bli enige om at godkjenningen forvaltes av én av dem. Det er da denne virksomheten som skal beskrives her.

|  |  |
| --- | --- |
| Virksomhetens navn |  |
| Forretningsadresse |  |
| Organisasjonsnummer  |  |
| Virksomhetens leder |  |
| Kontaktperson/stilling | Kontaktperson/stilling for godkjenningen |
| Kontaktinformasjon  | Kontaktinformasjon for kontaktpersonen |

## Informasjonssystem – systembeskrivelse

Informasjonssystemet identifiseres gjennom systembeskrivelse. Informasjon om systemet er del av grunnlaget for å avdekke sikkerhetsbehov og identifisere tiltakene som er nødvendige for å oppnå forsvarlig sikkerhetsnivå.

|  |  |
| --- | --- |
| Betegnelse  | "Systemnavn" el. også tidligere navn på systemet bør settes inn her. |
| Funksjon  | Overordnet beskrivelse av hvilke behov systemet dekker eller hvilke prosesser informasjonssystemet understøtter, eksempelvis:* kontorstøtte for behandling av gradert informasjon
* informasjonsutveksling av gradert informasjon med andre
* innsamling, sammenstilling og analyse av sensordata
* kommando og kontroll av operative enheter
 |
| Gradering / Klassifisering | Angivelse av høyeste gradering for informasjon som behandles i informasjonssystemet / høyeste klassifisering for objekt eller infrastruktur informasjonssystemet er utpekt som, eller har betydning for. |
| Teknologi  | Overordnet beskrivelse av informasjonssystemets teknologiske løsning og tekniske komponenter, eksempelvis informasjon om maskinvare, operativsystem, databaser og nettverkskomponenter. |
| Konfigurasjon  | Overordnet beskrivelse av informasjonssystemets utforming og sammenstilling, eksempelvis informasjon om tjenere, klienter perifert utstyr, og informasjon om deres sammenkobling. |
| Tjenester / Applikasjoner  | Overordnet beskrivelse av informasjonssystemets programvare, eksempelvis til bruk for funksjonene nevnt over. |

## Informasjonssystem – operativt miljø

Informasjonssystemets operative miljø utgjøres av de fysiske, elektroniske, menneskelig og organisatoriske forhold der systemet skal brukes. Informasjon om operativt miljø er del av grunnlaget for å avdekke sikkerhetsbehov og identifisere tiltakene som er nødvendige for å oppnå forsvarlig sikkerhetsnivå.

|  |  |
| --- | --- |
| Fysiske forhold | Overordnet beskrivelse av fysisk(e) område(r) der informasjonssystemet skal benyttes, eksempelvis faktisk lokalisering (adresse) eller typiske lokaliseringer som:* kontormiljø i Norge
* flyttbart for operativ bruk i felt
* norsk disponert område i utlandet
* kontrollert/beskyttet/sperret område
 |
| Elektroniske forhold | Overordnet beskrivelse av informasjonssystemets miljø for elektronisk håndtering og kommunikasjons av informasjon, eksempelvis (ekstern) dataoverføring og tilkoblinger til andre datasystemer. |
| Menneskelige forhold | Overordnet beskrivelse av mennesker i (tilsiktet) kontakt med informasjonssystemet, eksempelvis antall brukere. |
| Organisatoriske forhold | Overordnet beskrivelse av ansvars- og myndighetsfordeling for bruk, drift og vedlikehold av informasjonssystemet, eksempelvis oversikt over organisasjonstilhørighet for personell som drifter og (sikkerhets-)overvåker systemet. |

# Del 3 – Virksomhetens egen godkjenning

Godkjenning av skjermingsverdig informasjonssystem er en formell aktivitet, også når virksomheten selv er godkjenningsmyndighet. Virksomhetens godkjenningsmyndighet utøves av virksomhetens leder – med grunnlag i informasjonen i *Del 1* og *2* og etter å ha forsikret seg om at nødvendige sikkerhetstiltak er etablert.

Godkjenning av skjermingsverdig informasjonssystem kan gis for inntil 5 år[[3]](#footnote-3). Den bortfaller ved endringer som påvirker grunnlaget for godkjenningen.

Følgende bekreftelse signeres for skjermingsverdige informasjonssystemer virksomheten selv har godkjent. Del 3 gjelder derfor kun for informasjonssystemer som virksomheten selv kan godkjenne. Dersom NSM er godkjenningsmyndighet kan denne delen fjernes fra søknaden. Dersom virksomheten selv kan godkjenne, sendes erklæringen sammen med utfylt *Del 1* og *2* til NSM.

## Bekreftelse

*Undertegnede bekrefter at informasjonen i Del 1 og 2 er korrekt. Videre bekreftes at alle nødvendige sikkerhetstiltak for å oppnå forsvarlig sikkerhetsnivå, er etablert.*

*På dette grunnlag godkjennes informasjonssystemet inntil dd.mm.åå. Godkjenningen bortfaller dersom det oppstår vesentlig endring som har betydning for beskyttelsen av informasjonssystemet og informasjonen som behandles.*

|  |  |
| --- | --- |
| Sted og dato |  |
| Virksomhetens leder[[4]](#footnote-4) | Navn og signatur |

# Del 4 – Beskyttelsesbehov og sikkerhetstiltak

Forsvarlig sikkerhetsnivå oppnås ved å etablere nødvendige sikkerhetstiltak i forhold til beskyttelsesbehovet. Sikkerhetsbehov og tiltak fastlegges med grunnlag i informasjonssystemets systembeskrivelse og informasjon om operative miljø.

|  |  |
| --- | --- |
| Sikkerhetsgodkjenning etter hvilken § |  §52 / §54 (plan for lukking av avvik må være vedlagt ved søknad etter §54)  |
| Gjelder søknaden en re-godkjenning, **ny** midlertidig brukstillatelse eller er det tidligere er gitt dispensasjon fra virksomhetsikkerhetsforskriften §54 andre ledd? | JA / NEIHvis JA: beskriv kort de største endringer siden sist søknad.Er eventuelle forutsetninger/forbehold/vilkår i tidligere vedtak innfridd og dokumentert? |
| Behov for at NSM utsteder Statement Of Compliance (SOC) for systemet? | JA / NEIHvis JA: oppgi i hvilken periode |
| Sikkerhetstesting av informasjonssystemet er gjennomført og rapport som oppsummerer sikkerhetstesten er vedlagt søknaden? | JA/NEIHvis NEI: redegjør for fremdrift |

## Beskyttelsesbehov

Beskyttelsesbehovet beskrives ved å angi mulige og aktuelle scenarier det er nødvendig å beskytte seg mot for å oppnå forsvarlig sikkerhetsnivå.

|  |  |
| --- | --- |
| Beskytte data mot uønsket lesing og beskytte tjenester mot uønsket bruk | Scenarier som kan medføre uønsket lesing eller uønsket bruk, eksempelvis:Medarbeidere uten autorisasjon har tilgang til (skriver i, og) utskrifter fra det skjermingsverdige informasjonssystemet. |
| Beskytte data mot uønsket modifikasjon og beskytte tjenester mot uønsket modifikasjon og manipulasjon | Scenarier som kan medføre uønsket modifikasjon eller manipulasjon, eksempelvis:Eksterne har tilgang til informasjonssystemet gjennom tilkoblet system. |
| Beskytte data mot uønsket sletting og beskytte tjenester mot uønsket reduksjon eller stans | Scenarier som kan medføre uønsket sletting, uønsket reduksjon eller uønsket stans, eksempelvis:Eksternt vedlikeholds personell har tilgang til områder der informasjonssystemet er plassert og kan påvirke driften av systemet. |
| Identifisere 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 | Scenarier som kan medføre at brukere ikke identifiseres og autentiseres som (autoriserte) brukere før de gis tilgang: Eksempelvis:Tidligere ansatte benytter gamle påloggingsdata for å få tilgang til informasjonssystemet. |
| Forhindre at falske data og tjenester introduseres i informasjonssystemet | Scenarier som kan medføre at falske data eller tjenester introduseres i informasjonssystemet, eksempelvis:Ondsinnet programvare introduseres inn i systemet fra et annet sted enn via den eksternt rettede brannmuren, f.eks. via minnepenner eller andre flyttbare lagringsmedier. |
| registrere bruk, misbruk og forsøk på misbruk av informasjonssystemet, tjenester og data | Scenarier som kan medføre at bruk, misbruk eller forsøk på misbruk ikke registreres, eksempelvis:Teknisk registrering er iverksatt men sammenstilling og analyse av registreringene gjennomføres ikke i tilstrekkelig grad. |
| Systematisk kontrollere at sikkerhetstiltakene er korrekt implementert og ivaretar sikkerheten på en effektiv og hensiktsmessig måte | Scenarier som kan medføre at sikkerhetstiltak ikke kontrolleres, eksempelvis:Informasjonssystemet er ikke omfattet av virksomhetens program for interne sikkerhetsrevisjoner. |

## Sikkerhetstiltak – samsvar med tekniske veiledninger ("alternativ 1")

Sikkerhetstiltak kan velges med utgangspunkt i NSMs tekniske veiledninger. Veiledning velges i forhold til systembeskrivelse og informasjon om operative miljø og beskyttelsesbehov. Samsvar med teknisk(e) veiledning(er) dokumenteres og dokumentasjonen vedlegges søknad om godkjenning. *Vedlegg 1* gir eksempel på dokumentasjon av slik samsvarsvurdering. *Vedlegg 1* er unntatt offentligheten og kan anskaffes ved å henvende seg til NSM Postmottak.

## Sikkerhetstiltak – alternative tiltak ("alternativ 2")

Sikkerhetstiltak kan velges med utgangspunkt i vurdering av tilstrekkelighet og hensiktsmessighet i forhold til scenariene overfor sikkerhetsbehovet. Dette alternativet er nærmere beskrevet i NSMs *Veileder for godkjenning av informasjonssystem*. Tiltaksvurderingen vedlegges søknad om godkjenning. *Vedlegg 2* gir eksempel på dokumentasjon av slik vurdering. *Vedlegg 2* er unntatt offentligheten og kan anskaffes ved å henvende seg til NSM Postmottak.

## Sikkerhetstiltak – kombinasjon av samsvarsvurdering og tiltaksvurdering

Det er ikke utarbeidet tekniske veiledninger tilpasset alle systembeskrivelser, operative miljø og sikkerhetsbehov. Virksomheten kan dessuten velge å se bort fra deler av de tekniske veiledningene. Sikkerhetstiltak må da velges med utgangspunkt i samsvarsvurdering der det er mulig (eller ønskelig) og med utgangspunkt i tiltaksvurdering når dette er nødvendig (eller foretrekkes).

|  |  |
| --- | --- |
| Vedlagt ligger skisser over informasjonssystemet med dataflyt og eventuelle sammenkoblinger | JA / NEI |
| Vedlagt ligger beskrivelse av informasjonssystemet krypto | JA / NEI |
| Dersom andre krav er gjeldende (f.eks. NATO, FMN-krav) svares disse opp i vedlegg | JA/INGEN ANDRE KRAV ER GJELDENDE |
| Vi bekrefter med dette at systemet har oppnådd forsvarlig sikkerhet | JA/NEI |

**Nasjonal**

**sikkerhetsmyndighet**

Postboks 814

1306 Sandvika

postmottak@nsm.no

www.nsm.no

1. Både informasjonssystemer som skal behandle nasjonalt gradert informasjon og systemer som skal behandle NATO-gradert informasjon. [↑](#footnote-ref-1)
2. om ikke virksomheten likevel er gitt denne myndigheten [↑](#footnote-ref-2)
3. Informasjonssystemer som skal behandle NATO-gradert informasjon kan godkjennes for inntil 3 år. Slike systemer godkjennes (normalt) av NSM. [↑](#footnote-ref-3)
4. eller medarbeider med formell bemyndigelse fra virksomhetens leder til å godkjenne skjermingsverdige informasjonssystemer [↑](#footnote-ref-4)