Nasjonal sikkerhetsmyndighet

12.05.17

Veiledning i sikkerhetsgraderte anskaffelser og anskaffelser til kritisk infrastruktur

Fastsatt av Nasjonal sikkerhetsmyndighet med hjemmel i lov av 20. mars 1998 om forebyggende sikkerhetstjeneste (sikkerhetsloven) kapittel 7 med endringer, sist ved lov av 11. april 2008 og forskrift om sikkerhetsgraderte anskaffelser av 1. juli 2001.

Innhold

1 Innledning 3
2 Definisjoner og begrepsavklaringer 4
2.1 Sikkerhetsgradert anskaffelse 4
2.2 Bruker 4
2.3 Anskaffelsesmyndighet 4
2.4 Leverandør 4
2.5 Graderingsspesifikasjon 4
2.6 Personkontroll 5
2.7 Sikkerhetsklarering 5
2.8 Autorisasjon 5
2.9 Sikkerhetstruende virksomhet 5
2.10 Skjermingsverdig informasjon 6
2.11 Sikkerhetsgradert informasjon 6
2.12 Skjermingsverdig objekt 6
2.13 Kritisk infrastruktur 6
3 Gjennomføring av sikkerhetsgradert anskaffelse – ansvar, roller og krav 7
3.1 Bruker 7
3.2 Verdivurdering og graderingsspesifikasjon 7
3.3 Anskaffelsesmyndighet 8
3.4 Leverandør / underleverandør 9
3.5 Leverandørklarering 9
3.6 Sikkerhetsklarering av personell 11
3.7 Grunnlagsdokument for sikkerhet 12
3.8 Godkjenning av informasjonssystemer 13
3.9 Førstegangs inspeksjon 14
3.10 Sikkerhetsavtale 14
3.11 Autorisasjon 15
3.12 Utlevering av informasjon 16
3.13 Rapportering av sikkerhetstruende hendelser 16
3.14 Sikkerhetsmessig kontroll og oppfølging av leverandør 17
3.15 Terminering av anskaffelse 17
3.16 Spesielt om varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til kritisk infrastruktur 18
3.17 Utenlandske leverandører og anskaffelsesmyndigheter. 18
3.18 Besøksprosedyrer 19
3.19 Transport og forsendelse av sikkerhetsgradert informasjon 19
3.20 Transport og forsendelse av sikkerhetsgradert materiell 19
4 Vedlegg 20
Vedlegg 1 Henvisninger til styrende dokumenter og 20
veiledninger: 20
Vedlegg 2 Vanlige spørsmål 21
Vedlegg 3 Kontrollskjema 22
Vedlegg 4 Skjema til bruk i sikkerhetsgraderte anskaffelser 25

Veiledning i sikkerhetsgraderte anskaffelser og anskaffelser til kritisk infrastruktur

1 Innledning

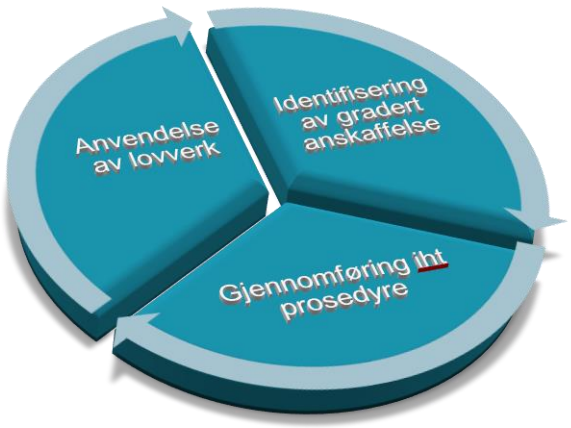
Sikkerhetsloven samt forskrifter inneholder et eget kapittel om sikkerhetsgraderte anskaffelser. Det er likevel viktig å merke seg at man må forholde seg til alle forskriftene i sikkerhetsloven når man arbeider med sikkerhetsgraderte anskaffelser.

Sikkerhetslovens definisjon av sikkerhetsgraderte anskaffelser beskriver en anskaffelsesprosess hvor blant annet leverandøren av varer og tjenester vil kunne få tilgang til skjermingsverdig informasjon eller objekt. Dette kan omfatte kjøp, leie og leasing. Målsetningen med regelverket for sikkerhetsgraderte anskaffelser er å ivareta beskyttelse av informasjon, materiell og objekt i tilknytning til ulike former for samhandel med virksomheter som ikke er forvaltningsorgan. Dette innebærer at regelverket også kommer til anvendelse ved salg, utleie og avhending.

En virksomhet som skal klareres som leverandør til sikkerhetsgraderte anskaffelser må tilfredsstille visse krav. Det kreves leverandørklarering for KONFIDENSIELT eller høyere. For nivå BEGRENSET kreves det ikke leverandørklarering, men det må likevel gjennomføres et forenklet kontrollregime da dette også er en sikkerhetsgradert anskaffelse.

Endringene i sikkerhetsloven som trådde i kraft 1. januar 2017 gir også noen føringer som gjelder anskaffelser til kritisk infrastruktur og overgang til tidsbestemt leverandørklarering. Dette er innarbeidet i denne veileder utgitt av Nasjonal sikkerhetsmyndighet (NSM).

Hensikten med denne veiledningen er å gi en oversikt over hvilke krav som stilles og hvordan prosedyrene gjennomføres. Ved bruk av malene som er utarbeidet for fagfeltet vil de formelle kravene gitt i sikkerhetsloven samt forskrift ivaretas.



2 Definisjoner og begrepsavklaringer

Sikkerhetsloven definerer sentrale begreper knyttet til sikkerhetsgraderte anskaffelser. Denne veilederen beskriver i tillegg andre begreper som også benyttes innen fagområdet.

2.1 Sikkerhetsgradert anskaffelse

Sikkerhetslovens § 3.
Sikkerhetsgradert anskaffelse; anskaffelse foretatt av anskaffelsesmyndighet som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker.

- Leverandøren vil få utlevert skjermingsverdig informasjon.
- Leverandøren må tilvirke skjermingsverdig informasjon.
- Informasjon om selve anskaffelsen må sikkerhetsgraderes.

2.2 Bruker

Med bruker menes den i en virksomhet som initierer en anskaffelse og som når denne er gjennomført skal disponere og drifte varen eller tjenesten frem til terminering.

- En bruker har det operative ansvaret for anskaffelsen, herunder å sørge for at den beskyttes sikkerhetsmessig gjennom hele dens levetid.

2.3 Anskaffelsesmyndighet

Sikkerhetslovens § 3.
Anskaffelsesmyndighet; et forvaltningsorgan som har til hensikt å anskaffe, eller allerede har anskaffet, varer eller tjenester fra rettssubjekt som ikke er forvaltningsorgan.

- Et forvaltningsorgan som på oppdrag fra en bruker har ansvar for å gjennomføre en anskaffelse

2.4 Leverandør

Forskrift om sikkerhetsgraderte anskaffelser § 1-2
Leverandør; et rettssubjekt som ikke er forvaltningsorgan og som leverer varer eller tjenester i forbindelse med en sikkerhetsgradert anskaffelse.

- Underleverandør er den som forestår leveranser til hovedleverandøren
- Underleverandører er sidestilt hovedleverandør sikkerhetsmessig

2.5 Graderingsspesifikasjon

Forskrift om sikkerhetsgraderte anskaffelser § 1-2
Graderingsspesifikasjon; en spesifisert liste over hvilke sikkerhetsgraderinger anskaffelsen omfatter.

- Graderingsspesifikasjon utarbeides på grunnlag av verdivurdering. Se for øvrig NSMs Veileder i verdivurdering og Håndbok i risikovurdering for sikring.
- Graderingsspesifikasjonen lister minimumsopplysninger som skal omfattes og hvilken

sikkerhetsgradering de ulike opplysningskategoriene har eller skal gis. Brukeren må selvstendig vurdere om det er behov for ytterligere opplysninger.

2.6 Personkontroll

Sikkerhetslovens § 3:
Personkontroll; innhenting av relevante opplysninger til vurdering av sikkerhetsklarering.

- Personkontroll gjennomføres i forbindelse med sikkerhetsklarering av personell.
- Ivaretas av Nasjonal sikkerhetsmyndighet etter anmodning fra klareringsmyndighet.

2.7 Sikkerhetsklarering

Sikkerhetslovens § 3:
Sikkerhetsklarering; avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad.

- Personell som skal gis tilgang til sikkerhetsgradert informasjon skal inneha en sikkerhetsklarering og være autorisert for det aktuelle graderingsnivået.
- Sikkerhetsklarering gis for KONFIDENSIELT nivå eller høyere. For BEGRENSET nivå benyttes bare autorisasjon etter at samtykke er innhentet hos klareringsmyndighet via anmodende myndighet. For utenlandske statsborgere se pkt 4.6.

2.8 Autorisasjon

Sikkerhetslovens § 3:
Autorisasjon; avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering, bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad.

- Autorisasjon på nivå BEGRENSET krever ikke forutgående sikkerhetsklarering.
- Anskaffelsesmyndigheten har ansvar for å autorisere virksomhetens leder
- Virksomhetens leder er ansvarlig for å autorisere eget personell som skal behandle/tilvirke sikkerhetsgradert informasjon/materiell i virksomhetens lokaler.
- Utenfor virksomhetens lokaler er det autorisasjonsansvarlig hos vedkommende virksomhet som skal autorisere innleid personell (f.eks. konsulenter).

2.9 Sikkerhetstruende virksomhet

Sikkerhetslovens § 3:
Sikkerhetstruende virksomhet; forberedelser til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger samt medvirkning til slik virksomhet.

- Sikkerhetstruende hendelser skal rapporteres, bevis skal sikres, rutiner skal gjennomgås, skadereduserende tiltak skal iverksettes, bakenforliggende årsaker skal fjernes slik at gjentakelse forhindres og reaksjon overfor ansvarlig person skal vurderes.
- Sikkerhetsbrudd og kompromittering av sikkerhetsgradert informasjon/materiell skal behandles og rapporteres.
- Rapport skal sendes til anskaffende myndighet som er gitt det sikkerhetsmessige ansvaret for virksomheten av NSM. Kopi av rapporten sendes til NSM. Virksomheten som er gitt det

sikkerhetsmessige ansvaret rapporterer videre til NSM eventuelt med flere.

2.10 Skjermingsverdig informasjon

Sikkerhetslovens § 3:
Skjermingsverdig informasjon; informasjon som skal merkes med sikkerhetsgrad etter reglene i sikkerhetslovens § 11.

- Sikkerhetsgradering fastsettes gjennom en verdivurdering.
- Både informasjon og materiell skal merkes med sikkerhetsgrad.
- Det er utsteder av skjermingsverdig informasjon som skal sørge for at informasjonen merkes med aktuell sikkerhetsgradering. Med utsteder menes virksomheten.

2.11 Sikkerhetsgradert informasjon

Sikkerhetslovens § 3:
Sikkerhetsgradert informasjon; informasjon som er merket med sikkerhetsgrad iht. reglene sikkerhetslovens § 11

- Både informasjon og materiell er merket med sikkerhetsgrad.
- Det er utsteder av sikkerhetsgradert informasjon som skal sørge for at informasjonen er merket med aktuell sikkerhetsgradering. Med utsteder menes virksomheten.

2.12 Skjermingsverdig objekt

Sikkerhetslovens § 3:
Skjermingsverdig objekt; eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser.

- Skjermingsverdige objekter utpekes av hvert enkelt departement innen sitt myndighetsområde.
- Skjermingsverdige objekter klassifiseres som VIKTIG, KRITISK eller MEGET KRITISK.
- Dersom fagdepartementet har fastsatt at det kreves sikkerhetsklarering for adgang til objektet benyttes følgende nivå:
  Objekt klassifisert KRITISK – Sikkerhetsklarering KONFIDENSIELT
  Objekt klassifisert MEGET KRITISK – Sikkerhetsklarering HEMMELIG eller høyere.

2.13 Kritisk infrastruktur

Sikkerhetslovens § 3:
Kritisk infrastruktur; anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner.

Direktoratet for samfunnssikkerhet og beredskap (DSB), Samfunnets kritiske funksjoner, høringsutgave september 2015, 85–86 fremstiller kritisk infrastruktur slik:

Matforsyning	Produksjonsanlegg, distribunaler, logistikksystemer, butikker
Vann og avløp	Vannverk, renseanlegg, pumper, høydebasseng
Sosiale ytelser og tjenester	NAVs it-systemer
Finansielle tjenester	Finansiell infrastruktur
Energiforsyning	Kraftverk, transformatorer, kraftnett osv. Fjernvarmeanlegg, pumpestasjoner, ledningsnett Raffinerier, havneanlegg, tankanlegg, bensinstasjoner
Elektronisk kommunikasjon	Kjernenett, transportnett, svitsjer
Transport	Veinett, jernbanelinjer, terminaler, trafikkstyringssystemer
Satellittbaserte tjenester	Satellitter, bakkestasjoner

3 Gjennomføring av sikkerhetsgradert anskaffelse – ansvar, roller og krav

Dette kapittelet beskriver ansvar, roller og krav knyttet til en sikkerhetsgradert anskaffelse. Veilederen omfatter i all vesentlighet tilstrekkelig informasjon til å kunne gjennomføre en sikkerhetsgradert anskaffelse. Det henvises likevel til sikkerhetsloven samt forskrifter for utfyllende informasjon.
Dette kapittelet bør leses i sammenheng med veilederens vedlegg 3. Vedlegg 3 viser en skjematisk fremstilling av prosessen, mens vedlegg 4 har forklarende tekst hentet fra dette kapittelet.

3.1 Bruker

Brukere av varer og tjenester initierer sikkerhetsgraderte anskaffelser og er ansvarlig for å gjennomføre verdivurdering og utarbeide graderingsspesifikasjon. I noen tilfeller kan anskaffelsesmyndigheten også være bruker. Dette gjelder blant annet i små virksomheter.

3.2 Verdivurdering og graderingsspesifikasjon

Forskrift om sikkerhetsgraderte anskaffelser § 2.1 sier: «Ved anskaffelser av varer og tjenester skal anskaffelsesmyndigheten vurdere behovet for å sikkerhetsgradere anskaffelsen eller deler av den». Anskaffelsesmyndigheten har ansvar for at det utarbeides verdivurdering og graderingsspesifikasjon med mindre det er en annen virksomhet som er bruker av varen eller tjenesten. Da er det denne (brukeren) som har ansvaret. Dersom det er flere brukere har anskaffelsesmyndigheten ansvaret for å utarbeide graderingsspesifikasjon for områder som er felles for brukerne. Brukeren av varen eller tjenesten skal når et behov oppstår igangsette en verdivurdering for å stadfeste om det er en sikkerhetsgradert anskaffelse eller ikke. Det er vesentlig at dette gjøres på et tidlig stadium slik at informasjon ikke allerede i starten blir kompromittert ved at sikkerhetsgradert informasjon fordeles eller lagres på informasjonssystemer som ikke tilfredsstiller nåværende eller

fremtidige sikkerhetskrav. Dette gjelder ikke minst når det gjelder innledende kontakt med potensielle leverandører eller konsulenter. Det må tas stilling til om det er behov for å utlevere sikkerhetsgradert informasjon til, eller at sikkerhetsgradert informasjon blir tilvirket hos, leverandør. Det kan også være nødvendig å sikkerhetsgradere anskaffelsen dersom informasjon om selve anskaffelsen må beskyttes. Verdivurderingen må ses i lys av hvilken skade det kan medfølge om ikke informasjonen sikres i tilstrekkelig grad. Gjennomføring av verdivurdering må involvere alle relevante aktører som direkte eller indirekte har interesser i anskaffelsen. Dersom anskaffelsen er en del av et større prosjekt kan det foreligge relevante risiko- og sårbarhetsvurderinger som må tas hensyn til. For utfyllende informasjon og verktøy for verdivurdering henvises til NSMs håndbok om sikringsrisikovurdering.

Dersom verdivurderingen konkluderer med at informasjon skal sikkerhetsgraderes skal det utarbeides en graderingsspesifikasjon som skal fremsendes anskaffelsesmyndigheten. Graderingsspesifikasjonen er å anse som en kravspesifikasjon for hvordan leverandøren sikkerhetsmessig skal forholde seg til mottatt og egentilvirket sikkerhetsgradert informasjon. Det kan i visse tilfeller oppstå endringer i sikkerhetsgraderingen av delelementer i en anskaffelse, og det er derfor viktig at man foretar endringer ved behov. Hele eller deler av anskaffelsen kan sikkerhetsgraderes.

Sikkerhetsgraderingsnivåer for følgende deler av anskaffelsen skal minimum være med:

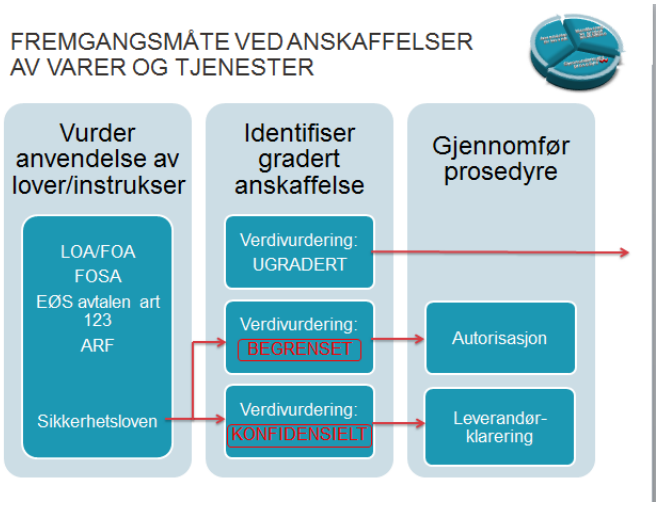
- Anbudsdokumenter.
- Kontrakten, kontraktsvilkår og kontraktsinngåelse.
- Tegninger og kravspesifikasjoner.
- Informasjon om enkeltkomponenter, faser, trinn ved anlegg og sammenstilling av enkeltkomponenter frem til endelig produkt.
- Andre aktuelle data, herunder eventuelle test- og ytelsesdata og lignende.
- Personell
- Informasjonssystem
- Eksistensen av anskaffelsen
- Det endelige resultatet.

Ved omfattende anskaffelser kan det være hensiktsmessig å dele opp flere av kulepunktene over i flere underkategorier som igjen kan ha ulik sikkerhetsgradering. Det kan gjøre det lettere å avgrense deler av anskaffelsen til f.eks. underleverandører og ulike informasjonssystemer.

3.3 Anskaffelsesmyndighet

Rollen som anskaffelsesmyndighet kan medføre at anskaffelsesmyndigheten blir utpekt til å ha det sikkerhetsmessige ansvar for leverandøren. Det er NSM som utpeker rollen som sikkerhetsmessig ansvarlig basert på blant annet hvilken anskaffelsesmyndighet som har størst sikringsbehov. Rollen innebærer rådgivning, veiledning, kontroll, godkjenning, anmodning, autorisasjon og oppfølging (tilsyn/inspeksjon) for å sikre en tilfredsstillende forebyggende sikkerhetstjeneste i henhold til sikkerhetslovens krav.

Det er anskaffelsesmyndigheten som velger leverandør og underleverandør(er) til en sikkerhetsgradert anskaffelse i henhold til de alminnelige bestemmelser som gjelder for forvaltningens anskaffelsesvirksomhet og brukerens behov. Anskaffelsesmyndigheten må ta stilling til om det i den aktuelle anskaffelsen er behov for å utveksle sikkerhetsgradert informasjon til leverandøren/ underleverandører for at denne skal ha selvstendig tilgang til denne. Dersom informasjonen som skal utveksles er sikkerhetsgradert KONFIDENSIELT eller høyere, kreves det leverandørklarering hvis vilkårene i kapittel nummer 2.1 er oppfylt. Det er NSM som er klareringsmyndighet i Norge for utstedelse av leverandørklareringer. Det er ikke krav om leverandørklarering for utlevering av informasjon sikkerhetsgradert BEGRENSET til leverandør/underleverandør(er). Det må likevel gjennomføres et forenklet kontrollregime da dette også er en sikkerhetsgrader anskaffelse. Anskaffelsesmyndigheten skal ved anbudsinnbydelse begrense spredning av sikkerhetsgradert informasjon til det som er høyst nødvendig. Sikkerhetsgradert informasjon skal ikke utleveres uten at det foreligger gyldig sikkerhetsavtale mellom anskaffelsesmyndighet og leverandør/ underleverandør(er).



3.4 Leverandør / underleverandør

Leverandørklarering skal foreligge før leverandøren / underleverandør gis tilgang til behandling av sikkerhetsgradert informasjon dersom vilkårene i punkt nummer 2.1 er oppfylt og sikkerhetsgraderingen er på KONFIDENSIELT nivå eller høyere. Leverandøren forholder seg sikkerhetsmessig til anskaffelsesmyndigheten. Dersom leverandøren innehar leverandørklarering for oppdrag for flere anskaffelsesmyndigheter skal NSM utpeke en av disse som sikkerhetsmessig ansvarlig overfor leverandøren. Hensikten med dette er å unngå at leverandøren må forholde seg til oppfølging og kontroll fra flere anskaffelsesmyndigheter, samtidig som unødig ressursbruk hos anskaffelsesmyndighetene unngås.

3.5 Leverandørklarering

Leverandørklarering skal foreligge for anskaffelser på KONFIDENSIELT nivå eller høyere. Leverandørklarering gis for en periode på 5 år. Anskaffelsesmyndigheten skal forespørre NSM om aktuell leverandør innehar en gyldig leverandørklarering. Dette gjøres på eget skjema (vedlegg B). Dersom leverandøren innehar en leverandørklarering vil NSM gi denne opplysningen til

anskaffelsesmyndigheten på blankettens del 2. Det vil også opplyses om hvilken anskaffelsesmyndighet som er sikkerhetsmessig ansvarlig. Dersom leverandøren ikke innehar en leverandørklarering må anskaffelsesmyndighet sende anmodning til NSM om å iverksette leverandørklarering. Anmodningen skal inneholde graderingsspesifikasjon og egenopplysningsblankett fra leverandør. Anskaffelsesmyndigheten vil deretter motta et vedtaksbrev. Dersom leverandørklarering gis vil det eventuelt opplyses om anmodende myndighet skal være sikkerhetsmessig ansvarlig. En leverandørklarering gjelder bare for den av leverandørens lokasjoner det er anmodet om leverandørklarering for. Dette fremgår av besøksadresse (og organisasjonsnummer dersom denne er enestående for denne adresse).

Minimumskrav til egenopplysninger:

- Navn (firma), adresse og eierform.
- Utenlandske eierinteresser hos leverandøren med angivelse av nasjonalitet.
- Leverandørens eierinteresser i utlandet med angivelse av nasjonalitet.
- Norske og utenlandske statsborgere i leverandørens styre (herunder varamedlemmer) og leverandørens ledelse med navn, fødselsdato og nasjonalitet. (Fødselsnummer for norske statsborgere og fødselsdato for utenlandske statsborgere.)
- Oppdrag for utenlandske oppdragsgivere.
- Utenlandshandelens størrelse av total årsomsetning.
- Næringsinteresser som personer i leverandørens styre og ledelse har i utlandet.
- Utenlandske statsborgere hos leverandøren som har behov for tilgang til sikkerhetsgradert informasjon.
- Besøksadresse og skisse/tegninger for de lokaler som er tenkt benyttet ved anskaffelsen.

Leverandørklarering kan termineres dersom leverandøren ikke lenger anses sikkerhetsmessig skikket.

NSM, eller den anskaffelsesmyndigheten NSM utpeker, er sikkerhetsmessig ansvarlig for norske leverandører til utenlandske myndigheters sikkerhetsgraderte anskaffelser. Leverandører sender personopplysningsblanketten med leverandørvedlegg til respektive anmodende myndighet. Denne videresender personopplysningsblanketten til rette klareringsmyndighet.

På BEGRENSET nivå trenger ikke anskaffelsesmyndigheten å søke NSM om tillatelse / leverandørklarering. Det kreves likevel at anskaffelsesmyndigheten forsikrer seg om at leverandøren er sikkerhetsmessig skikket til å oppbevare, behandle og tilvirke sikkerhetsgradert informasjon/materiell.

Forhold som blir vurdert under leverandørklareringsprosessen

- Økonomiske forhold, herunder muligheten for insolvens (kredittverdighet).
- Eierform og eierinteresser.
- Sikkerhetsmessige forhold for daglig leder og styre.
- Sikkerhetsorganisasjonen.
- Gjennomføring av forebyggende sikkerhet.
- Mulige straffbare forhold, herunder forhold som kan kvalifisere til foretaksstraff.
- Andre forhold som kan gi grunn til å frykte at leverandøren vil kunne opptre i strid med sikkerhetsmessige interesser.

.

3.6 Sikkerhetsklarering av personell

Leverandør/underleverandør(er) som innehar leverandørklarering skal sende personopplysningsblankett med leverandørvedlegg til anskaffelsesmyndigheten. Anskaffelsesmyndigheten anmoder klareringsmyndigheten om sikkerhetsklarering av leverandørens personell. Leverandørens daglige leder og styremedlemmer samt øvrig personell som kan få tilgang til sikkerhetsgradert informasjon skal sikkerhetsklareres. Dersom det ikke er mulig eller nødvendig å gi et styremedlem sikkerhetsklarering skal erklæring om fraskrivelse av innsynsrett innhentes. Fraskrivelse signeres på to eksemplarer, hvorav ett sendes anskaffelsesmyndighet og beholdes hos leverandøren. Anskaffelsesmyndigheten sender kopi til NSM.

Før tilgang til sikkerhetsgradert informasjon/materiell kan gis, skal vedkommende være sikkerhetsklarert og autorisert. Ved tilgang til informasjon sikkerhetsgradert BEGRENSET kreves ikke forutgående sikkerhetsklarering, men autorisasjon etter samtykke fra vedkommende klareringsmyndighet.

Dersom en anskaffelse gjennomføres ved at leverandørens personell utelukkende løser oppdraget i anskaffelsesmyndighetens lokaler kreves det kun sikkerhetsklarering av personellet. I slike tilfeller er det anskaffelsesmyndigheten som autoriserer personellet.

Ved utfylling av personopplysningsblanketten (X-0136/1B) er det viktig at «Veiledning til utfylling av personopplysningsblankett» blir brukt. Autorisasjonsansvarlig skal ved utlevering av blanketten opplyse om hvilket sikkerhetsklareringsnivå vedkommende skal sikkerhetsklareres for.

- Forskrift om personellsikkerhet gjelder fullt ut.
- Punktene 2 til 25 på personopplysningsblanketten fylles ut etter gitt klareringsnivå av vedkommende det skal søkes sikkerhetsklarering for og vedkommende legger den i forseglet konvolutt. Punkt 1 fylles ut av anskaffelsesmyndighet.
- Leverandøren fyller ut Leverandørvedlegg med begrunnelse for klareringsanmodningen og sender denne og forseglet konvolutt med personopplysningsblankett til anskaffelsesmyndigheten.
- Ved mottak hos anskaffelsesmyndighet påføres personopplysningsblanketten og saksomslaget sikkerhetsgraderingsnivå etter innhold (minimum BEGRENSET). Dersom informasjonen er mangelfull skal den returneres til vedkommende som da må rette opp manglene. Leverandør og anskaffelsesmyndigheten skal føre journal for egen saksbehandling.
- En rekke anskaffelsesmyndigheter er også klareringsmyndigheter for sikkerhetsklarering av personell.
- Klareringsmyndigheten innhenter personkontrollopplysninger fra NSM, og ved behov ytterligere opplysninger, og foretar en klareringsavgjørelse på grunnlag av mottatte opplysninger. Klareringsmyndigheten underretter anskaffelsesmyndigheten om klareringsavgjørelsen, eventuelt leverandøren direkte dersom anskaffelsesmyndighet er klareringsmyndighet.
- Etter mottak av klareringsavgjørelsen sender anskaffelsesmyndigheten personopplysningsblanketten og klareringsbevis i saksomslag til leverandøren forutsatt at leverandøren har gyldig sikkerhetsavtale på minimum BEGRENSET nivå.
- Saksomslaget (blankett S-0136/5) skal inneholde original personopplysningsblankett, klareringsbevis, taushetserklæring og samtaleskjema hos autorisasjonsansvarlig eller den vedkommende bemyndiger. Saksomslaget skal oppbevares adskilt fra andre

arkivdokumenter.
- Det er viktig at forsendelser merkes med rett adressat slik at ikke saksgangen forlenges på grunn av feilsending.

Anskaffelser der en hovedleverandør med leverandørklarering benytter personell fra underleverandører som kun skal ha tilgang til sikkerhetsgradert informasjon/materiell hos hovedleverandør, medfører en noe annen rutine:

- Aktuelt personell hos underleverandøren fyller ut personopplysningsblanketten.
- Blanketten sendes til autorisasjonsansvarlig hos hovedleverandøren (i lukket konvolutt merket med navn og fødselsdato på vedkommende) som videresender den til anskaffelsesmyndigheten med utfylt og signert Leverandørvedlegg.
- Klareringsbevis og original personopplysningsblankett sendes i saksomslag fra anskaffelsesmyndighet til hovedleverandør som oppbevarer disse.
- Sikkerhetsmessig betraktes dette personellet som tilhørende hos hovedleverandøren.
- Underleverandøren skal ikke ha tilgang til opplysningene gitt på blanketten.

Utenlandsk statsborger kan gis sikkerhetsklarering etter en vurdering av hjemlandets sikkerhetsmessige betydning og vedkommendes tilknytning til hjemlandet og Norge. Sikkerhetslovens § 2-2. gir føringer for sikkerhetsklarering og autorisasjon av utenlandske statsborgere herunder:

- Sikkerhetsklarering og autorisasjon av utenlandske statsborgere kan bare gjøres gjeldende for tilgang til norsk sikkerhetsgradert informasjon.
- Tilgang til fremmede staters tilsvarende informasjon kan bare gis dersom vedkommende er borger av denne stat eller tillatelse er gitt av statens kompetente myndigheter.
- Tilgang til informasjon sikkerhetsgradert av eller tilhørende en internasjonal organisasjon kan bare gis dersom staten vedkommende er borger av er medlem av organisasjonen, eller organisasjonen har gitt tillatelse til det.
- Virksomhet som har behov for å autorisere utenlandske statsborgere, kan bare autorisere etter at tillatelse er innhentet fra vedkommende departement i hvert enkelt tilfelle.
- Før autorisasjon gis for tilgang til informasjon gradert KONFIDENSIELT eller høyere skal vedkommende inneha norsk sikkerhetsklarering.
- Personer som er statsløse eller har dobbelt statsborgerskap, skal sikkerhetsklareres og autoriseres etter bestemmelsene for utenlandske statsborgere.
- Egne prosedyrer for autorisasjon for BEGRENSET

3.7 Grunnlagsdokument for sikkerhet

Virksomheter med sikkerhetsgradert informasjon skal ha et ajourført Grunnlagsdokument for sikkerhet (GDS) som skal identifisere grunnleggende forutsetninger for virksomhetens håndtering av skjermingsverdig informasjon. Dersom leverandører får utlevert eller skal tilvirke sikkerhetsgradert informasjon skal grunnlagsdokument for sikkerhet foreligge uansett graderingsnivå.

Grunnlagsdokument for sikkerhet skal beskrive:

- Sikkerhetsorganisasjon og dens myndighet.
- Sikkerhetsmessig inndeling i fysiske områder ved virksomheten, og hvor sikkerhetsgradert informasjon tillates behandlet og oppbevart med angivelse av høyeste sikkerhetsgrad.
- Hvilke informasjonssystemer, herunder kryptosystemer, som håndterer sikkerhetsgradert informasjon, med angivelse av hvilken sikkerhetsgrad hvert system er godkjent for og i hvilke fysiske område det enkelte system er plassert.
- Oversikt over kommunikasjon av sikkerhetsgradert informasjon som er etablert internt i virksomheten og mot andre virksomheter.
- Hvem som har behov for tilgang til hvilke type sikkerhetsgradert informasjon med tilhørende informasjonssystemer.
- Planer, instrukser, prosedyrer og annen dokumentasjon for sikkerhet, herunder relevant dokumentasjon og sikkerhetsfaglig kompetanse og kompetansebygging iht kapittel 3 i sikkerhetsloven.

Informasjon som er sikkerhetsgradert bør utarbeides som vedlegg til GDS slik at øvrig informasjon er lett tilgjengelig for autorisert personell.

3.8 Godkjenning av informasjonssystemer

I mange tilfeller har anskaffelsesmyndigheten behov for at leverandører behandler sikkerhetsgradert informasjon elektronisk i forbindelse med en sikkerhetsgradert anskaffelse.
Sikkerhetslovens § 13 fastsetter at alle virksomheter som behandler sikkerhetsgradert informasjon elektronisk skal ha sikkerhetsgodkjente informasjonssystemer for håndtering av denne type informasjon. Sikkerhetsgodkjenning skal foreligge før informasjonssystemet benyttes til håndtering av sikkerhetsgradert informasjon. Det er NSM, eller den som NSM utpeker, som foretar sikkerhetsgodkjenningen av informasjonssystemet. Dette gjøres med bakgrunn i blant annet valgt operasjonsmåte, sikkerhetsgradering og eksterne forbindelser. I de tilfeller hvor det er anskaffende myndighet som gir sikkerhetsgodkjenningen skal anskaffende myndighet sende kopi av godkjenningsskriv til NSM.

For sikkerhetsgraderte informasjonssystemer hos leverandører på nivå KONFIDENSIELT eller høyere, skal det utarbeides en TEMPEST risikovurdering.

- Med TEMPEST menes elektromagnetisk stråling fra elektronisk utstyr som utilsiktet kan forårsake at uvedkommende kan få tilgang til sikkerhetsgradert informasjon.
- Begrepet benyttes også om undersøkelser og analyser knyttet til slike fenomener.

Det skal eventuelt iverksettes tiltak for beskyttelse mot at uvedkommende kan få tilgang til sikkerhetsgradert informasjon ved å motta og analysere kompromitterende elektromagnetisk stråling. Tempestrisikovurderingen skal fremsendes anskaffende myndighet eller NSM for kontroll. Anskaffende myndighet skal vurdere behov for beskyttelsestiltak, herunder for eksempel kryptering ved elektronisk utveksling av sikkerhetsgradert informasjon mellom flere virksomheter. Informasjonssystemer og maskinlesbare lagringsmedium som er personlig eid skal ikke benyttes til

håndtering av sikkerhetsgradert informasjon. (Lagringsmedium kan eksempelvis være harddisker inkludert SSD og minnepinner).

3.9 Førstegangs inspeksjon

For anskaffelser på KONFIDENSIELT nivå eller høyere kreves det at det er gjennomført en inspeksjon hos leverandør før sikkerhetsavtale inngås. Det er ikke krav om dette på BEGRENSET nivå, men det kan være hensiktsmessig å gjøre det likevel da det blir letter å vurdere virksomhetens skikkethet til å ivareta sikkerheten. En slik inspeksjon kan også benyttes til å gjennomføre autorisering av daglig leder.

Det er utarbeidet en mal som angir hovedpunktene som inngår i rapport etter sikkerhetsinspeksjon hos leverandør. Normalt vil rapporten bli gradert BEGRENSET eller Unntatt offentlighet.

3.10 Sikkerhetsavtale

Sikkerhetsavtale skal inngås på nivå BEGRENSET eller høyere. Sikkerhetsavtalen formaliserer sikkerhetsmessige aspekter i forbindelse med anskaffelsen.

Forskrift om sikkerhetsgraderte anskaffelser regulerer hva som minimum skal være med i en sikkerhetsavtale. Ved anskaffelser der det kreves leverandørklarering skal sikkerhetsavtalen i tillegg regulere forhold vedrørende sikkerhetsklarering av personell og endringer i eierinteresser eller eierform hos leverandøren.

Sikkerhetsavtale skal utarbeides av anskaffelsesmyndigheten. Avtalen er gyldig når den er undertegnet av både leverandørens daglige leder og anskaffelsesmyndighetens leder. Myndigheten til å signere avtalen kan skriftlig delegeres av begge parter. Anskaffelsesmyndighet har ansvar for å fremsende kopi av sikkerhetsavtale med graderingsspesifikasjon til Nasjonal sikkerhetsmyndighet.

Innholdet i en sikkerhetsavtale:

- Anskaffelsens navn og sikkerhetsgradering med graderingsspesifikasjon.
- Innhenting av sikkerhetsklarering, taushetserklæring fra og autorisasjon av personell hos leverandøren som kan få tilgang til sikkerhetsgradert informasjon.
- Utlevering og bekjentgjøring av skjermingsverdig informasjon til tredjepart, herunder til underleverandører, konsulenter, målgrupper for markedsføring og media.
- Forvaltning av sikkerhetsgradert informasjon, herunder eventuell godkjenning for bruk av informasjonssystemer og tilbakelevering av lagringsmedier.
- Omkostninger ved sikkerhetstiltak.
- Flytting av lokaler som krever ny sikkerhetsmessig godkjenning.
- Endringer i styre, endring av daglig leder og endring av firmanavn.
- Tilbakelevering av sikkerhetsgradert informasjon ved utløp av eventuell anbudsfrist og ved oppdragets slutt.
- Rutiner for varsling og tiltak ved insolvens, gjeldsforhandlinger og konkurs.
- Rett til sikkerhetsinspeksjoner for anskaffelsesmyndighet og/eller NSM.
- Spesielle vilkår.
- Sikkerhetsavtalens gyldighetstid.
- Endringer i sikkerhetsavtalen.

Dersom det ved en feiltakelse ikke er inngått en sikkerhetsavtale, er leverandøren likevel forpliktet til å følge sikkerhetsloven. Anskaffelsesmyndigheten må, iht. sikkerhetsloven, snarest få en avtale på plass når dette oppdages.

3.11 Autorisasjon

Autorisasjon og undertegning av taushetserklæring er en forutsetning for å kunne motta sikkerhetsgradert informasjon. Anskaffelsesmyndigheten har et spesielt ansvar for å autorisere leverandørens daglige leder.

Forutsetningen for å gi autorisasjon:

- Vedkommende innehar nødvendig sikkerhetsklarering unntatt BEGRENSET.
- Det foreligger et tjenstlig behov for å gi vedkommende tilgang til sikkerhetsgradert informasjon.
- Taushetserklæring er undertegnet.
- Vedkommende kjenner de aktuelle sikkerhetsbestemmelsene.
- Autorisasjonssamtale er gjennomført.
- Det ikke foreligger opplysninger som gjør det tvilsomt om vedkommende er sikkerhetsmessig til å stole på.
- Identitetskontroll er foretatt.

Leverandører skal selv autorisere eget personell for BEGRENSET nivå etter samtykke fra klareringsmyndigheten. Dette gjelder også for underleverandører. Autorisasjon for BEGRENSET medfører ikke forutgående sikkerhetsklarering.

Leverandører med leverandørklarering (KONFIDENSIELT eller høyere):

- Anskaffelsesmyndigheten autoriserer leverandørens daglige leder.
- Daglig leder autoriserer så øvrig personell hos leverandøren i samsvar med forskrift om personellsikkerhet kapittel 5. NSMs «Håndbok i autorisasjonssamtale» anbefales benyttet.
- På saksomslag for personellsikkerhet (blankett S0136/5) påføres det at autorisasjonssamtale er gjennomført (av hvem og når) og at autorisasjon er gitt (dato, nivå og av hvem).
- Taushetserklæring skal fylles ut og underskrives.
- Samtaleskjema er gjennomgått og undertegnet av begge parter.

Autorisasjonssamtale gjennomføres for å avklare tillitsforholdet mellom autorisasjonsansvarlig og personell som skal ha tilgang til sikkerhetsgradert informasjon.

Autorisasjonssamtale skal gjennomføres:

- Før autorisasjon finner sted.
- Når vedkommende person selv ønsker det.
- Ved reklarering.
- Når autorisasjonsansvarlig ellers finner grunn til det.

Dersom en person utfører konsulenttjenester hos flere anskaffelsesmyndigheter autoriseres vedkommende av hver enkelt anskaffelsesmyndighet.

3.12 Utlevering av informasjon

Før sikkerhetsgradert informasjon kan utleveres eller tilvirkes av leverandør må visse vilkår være oppfylt. Utgangspunktet er at det foreligger behov for en sikkerhetsgradert anskaffelse.

Dersom personellet som utfører oppdraget gjør dette utelukkende i anskaffelsesmyndighetens lokaler kreves det ikke leverandørklarering men kun sikkerhetsklarering av personell.

Kriterier for utlevering nivå KONFIDENSIELT eller høyere når det kreves leverandørklarering:

- Leverandøren skal inneha leverandørklarering dersom vilkårene for dette er oppfylt.
- Signert sikkerhetsavtale med graderingsspesifikasjon skal foreligge for den aktuelle anskaffelsen. Kopi skal være sendt NSM.
- Leverandøren er kjent med aktuelle sikkerhetsbestemmelser.
- Personellet leverandøren skal benytte skal være sikkerhetsklarert og autorisert i samsvar med sikkerhetslovens § 19.
- Det skal ikke foreligge opplysninger som gjør det tvilsomt om leverandøren er sikkerhetsmessig skikket.
- Firmaattest fra foretaksregisteret eller enhetsregisteret skal foreligge for kontroll av identitet og grunnleggende opplysninger om leverandøren.

Det er ikke krav til leverandørklarering ved utlevering av informasjon gradert BEGRENSET. Anskaffelsesmyndigheten treffer selv avgjørelse om utlevering.

Kriterier for utlevering nivå BEGRENSET:

- Signert sikkerhetsavtale med graderingsspesifikasjon skal foreligge for den aktuelle anskaffelsen. Kopi skal være sendt NSM.
- Daglig leder og aktuelt personell hos leverandøren skal ha undertegnet taushetserklæring, gjennomført autorisasjonssamtale og være autorisert.
- Dersom styremedlemmer krever innsyn i informasjon gradert BEGRENSET skal disse autoriseres etter samtykke fra klareringsmyndigheten. Utenlandske statsborgere kan eventuelt autoriseres iht. forskrift om personellsikkerhet § 2-2.
- Grunnlagsdokument for sikkerhet (GDS) samt andre instrukser, prosedyrer og stillingsbeskrivelser skal foreligge.
- Leverandøren skal oppfylle kravene iht. forskrift om informasjonssikkerhet.

3.13 Rapportering av sikkerhetstruende hendelser

Ved sikkerhetstruende hendelser skal skadereduserende tiltak skal iverksettes umiddelbart, bevis skal sikres, hendelsen skal rapporteres, underliggende årsaker skal identifiseres, tiltak for å hindre gjentakelse skal iverksettes og reaksjon overfor ansvarlig person skal vurderes.

Leverandører skal rapportere om sikkerhetstruende hendelser/sikkerhetsbrudd og om forhold som reiser tvil om den sikkerhetsmessige skikkethet til noen som har befatning med den sikkerhetsgraderte anskaffelsen.

Sikkerhetsbrudd og kompromittering av sikkerhetsgradert informasjon skal behandles og rapporteres internt iht. virksomhetens risikohåndteringsverktøy. Rapportering skal foretas til den virksomheten som har det sikkerhetsmessige ansvaret for leverandøren, eieren av den sikkerhetsgraderte informasjonen, andre virksomheter som dette har betydning for samt NSM. Det skal vurderes om forholdet skal anmeldelse til politiet.

Ved kompromittering av informasjon sikkerhetsgradert KONFIDENSIELT eller høyere skal virksomheten som tilvirket informasjonen utarbeide skadevurdering.

3.14 Sikkerhetsmessig kontroll og oppfølging av leverandør

Anskaffelsesmyndigheten skal gjennom sikkerhetsinspeksjoner og oppfølging forsikre seg om at leverandører og underleverandører det er inngått sikkerhetsavtale med oppfyller krav fastsatt i sikkerhetsloven samt forskrifter.

- Kontroll utøves ved sikkerhetsinspeksjoner og skal gjennomføres jevnlig og minst en gang hver 18. måned i løpet av anskaffelsen.
- De delene av sikkerhetsloven samt forskrifter som er relevante for anskaffelsen omfattes av inspeksjonen.
- Anskaffelsesmyndigheter kan pålegge underordnede anskaffelsesmyndigheter eller bemyndige andre anskaffelsesmyndigheter å utføre inspeksjon dersom dette er hensiktsmessig.
- Anskaffelsesmyndigheten skal utarbeide inspeksjonsrapport som skal formidles leverandøren med kopi til NSM. Rapporten skal angi avvik med pålegg om lukking av disse.
- Avvik skal lukkes innen tidsfrist.
- NSM er ansvarlig for at alle norske anskaffelsesmyndigheter som har sikkerhetsavtale med leverandøren får tilsendt kopi av rapporten eller deler av den.

3.15 Terminering av anskaffelse

Terminering av anskaffelse innebærer avslutning av anskaffelsen, tilbakelevering av sikkerhetsgradert informasjon og materiell, tilbakekalling av sikkerhetsgodkjenning av informasjonssystem og terminering av sikkerhetsavtalen. Det må vurderes om det skal inngås en ny sikkerhetsavtale dersom det er behov for videre avtaler som omfatter for eksempel service og vedlikehold.

- All sikkerhetsgradert informasjon, utstyr og materiell knyttet til anskaffelsen skal trekkes tilbake av anskaffelsesmyndigheten med mindre NSM eller den NSM bemyndiger samtykker i annet.
- Ved behov iverksetter anskaffelsesmyndigheten kontroll hos leverandøren for å sikre at alt sikkerhetsgradert informasjon og materiell er tilbakelevert eller etter samtykke fra informasjonseier destruert. Dette skal gjennomføres før sikkerhetsavtalen termineres

- NSM skal være kopiadressat når en sikkerhetsavtale termineres.

3.16 Spesielt om varslingsplikt og myndighet til å fatte vedtak ved anskaffelser til kritisk infrastruktur

Sikkerhetslovens § 29 a omhandler kritisk infrastruktur som defineres som; anlegg og systemer som er nødvendige for å opprettholde samfunnets grunnleggende behov og funksjoner.

- Ved anskaffelser til kritisk infrastruktur skal det foretas en risikovurdering. I vurderingen skal det tas stilling til om anskaffelsen innebærer en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført mot eller ved bruk av infrastrukturen.
- Ved gjennomføring av risikovurdering vil det være hensiktsmessig å benytte en metode som forholder seg til villede uønskede handlinger
- NSMs håndbok i risikovurdering for sikring gir en innføring i denne metodikken
- En virksomhet som eier eller rår over kritisk infrastruktur, skal varsle overordnet departement dersom en risikovurdering som nevnt i første ledd konkluderer med at anskaffelsen kan innebære en ikke ubetydelig risiko for at sikkerhetstruende virksomhet blir etablert eller gjennomført. Virksomheter som ikke er underlagt noe departement, skal varsle Forsvarsdepartementet.

3.17 Utenlandske leverandører og anskaffelsesmyndigheter.

Prosedyrer knyttet til sikkerhetsgraderte anskaffelser som involverer utenlandske leverandører og anskaffelsesmyndigheter er regulert i bilaterale avtaler, og samarbeidsformer gitt i MISWG rammeverket (Multinational Industrial Security Working Group) og NATO AC3.

Når utenlandske myndigheter eller virksomheter vil benytte norske leverandører vil NSM motta en anmodning fra utenlandsk sikkerhetsmyndighet.

- NSM gir tilbakemelding på eventuell klareringsstatus på omspurte leverandør.
- Dersom leverandøren ikke innehar en leverandørklarering vil NSM på oppfordring fra anmodende utenlandsk sikkerhetsmyndighet igangsette klareringsprosess.
- NSM kan da få rollen som sikkerhetsmessig ansvarlig for leverandøren og fører kontroll med leverandøren på utenlandsk sikkerhetsmyndighets vegne.

Når utenlandsk leverandør ønskes benyttet i en sikkerhetsgradert anskaffelse, fremmer den norske anskaffelsesmyndigheten en anmodning til NSM som skal inneholde graderingsspesifikasjon på engelsk.

- Når anskaffelsesmyndigheten har fått tillatelse til utlevering av norsk sikkerhetsgradert informasjon til utenlandsk leverandør inngår denne sikkerhetsavtale (Security Clauses) med den utenlandske leverandøren.

- En rekke nasjoner benytter ikke ekvivalenten til norsk BEGRENSET og gir derfor ikke informasjon når forespørselen er på dette nivået. I slike tilfeller må sikkerheten ivaretas gjennom merkantile avtaler.
- Anskaffelsesmyndigheten skal etter signatur formidle kopi av Security Clauses til NSM som vil informere den respektive kompetente nasjonale sikkerhetsmyndigheter om at anskaffelsen har blitt iverksatt.
- Utenlandsk sikkerhetsmyndighet vil føre tilsyn med leverandøren på NSMs vegne.

3.18 Besøksprosedyrer

Det enkelte departement er ansvarlig for å gjennomføre besøkskontroll innen eget ansvars- og myndighetsområde. NSM har utpekt Forsvarets sikkerhetsavdeling (FSA) til å ivareta besøkskontroll for forsvarssektoren med tilhørende sivile virksomheter/ leverandører. Det skal benyttes eget skjema ved besøk til fremmede stater eller internasjonale organisasjoner Norge har sikkerhetsavtale med. Norge har gjennom overenskomster med en rekke stater og organisasjoner forpliktet seg til å bruke dette skjema ved internasjonale besøk knyttet til sikkerhetsgraderte anskaffelser.
Se vedlegg I.

3.19 Transport og forsendelse av sikkerhetsgradert informasjon

Kurerposttjeneste innen Norges grenser kan bare utføres av Forsvaret eller annen virksomhet godkjent av NSM for dette formålet. Kurerposttjenester i eller til fremmede stater kan bare utføres av utenrikstjenesten, Forsvaret eller annen virksomhet godkjent av NSM for dette formålet. All kurertjeneste skal utføres i henhold til forskrift om sikkerhetsadministrasjon kapittel 8.

- Som kurer kan bare benyttes person som er offentlig tjenestemann, ansatt i virksomhet godkjent av NSM for kurerposttjeneste, eller som er godkjent av Utenriksdepartementet, Forsvaret eller NSM.
- Ved kurerforsendelse skal avsender utstede kurersertifikat.
- NSM utsteder kurersertifikat for personell som ikke er offentlige tjenestemenn, men som er godkjent av NSM.
- Foreign Handcarry Worksheet benyttes i de tilfeller kureren(e) til enhver tid kan ha kontroll på materiellet. Dette gjelder som regel mindre kolli som kureren har i sin varetekt.

3.20 Transport og forsendelse av sikkerhetsgradert materiell

Ved forsendelse av sikkerhetsgradert materiell til og fra fremmede stater i forbindelse med salg eller kjøp av varer skal det utarbeides en transportplan. Norske leverandører eller myndigheter fremsender transportplan til NSM når det er mottakeren er utenlandsk. Transportplanen skal godkjennes av de utenlandske sikkerhetsmyndigheter som blir berørt av forsendelsen.

- Transportation plan for the movement of classified material as freight (MISWG Document number 10 Appendix S) benyttes ved transport av større kolli.

Det er viktig å starte arbeidet med transportplan på et tidlig tidspunkt i prosessen da saksgangen kan ta tid, spesielt hvis flere stater er involvert. En transport kan ikke igangsettes før NSM har gitt tillatelse og kurersertifikater er utstedt.

Ved transporter i Forsvarets regi kreves det ikke transportplan dersom dette skjer government til government.

4 Vedlegg

Vedlegg 1 Henvisninger til styrende dokumenter og veiledninger:

http://lovdata.no

1. Sikkerhetsloven § 3 nummer 16-17 og kapittel 7 (§§ 27-29) samt forskrift om sikkerhetsgraderte anskaffelser av 1. juli 2001 nr. 753.
2. Forskrift om sikkerhetsadministrasjon
3. Forskrift om personellsikkerhet
4. Forskrift om informasjonssikkerhet
5. Forskrift om sikkerhetsgraderte anskaffelser

https://www.nsm.stat.no/Publikasjoner/regelverk/Veiledninger/

1. Veiledning i sikkerhetsstyring
2. Veiledning i verdivurdering
3. Veiledninger i systemteknisk sikkerhet
4. Veiledning for informasjonssystemsikkerhet
5. Veiledning i objektsikkerhet
6. Veiledning for sikkerhetsgraderte anskaffelser med skjema
7. Veiledning i personellsikkerhet

Vedlegg 2 Vanlige spørsmål

Hva er en sikkerhetsgradert anskaffelse? Det er en anskaffelse foretatt av en anskaffelsesmyndighet som medfører at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, vil kunne måtte tilvirke skjermingsverdig informasjon eller at anskaffelsen må skjermes av andre årsaker.
Hva er en anskaffelsesmyndighet? Ethvert forvaltningsorgan i stat eller kommune, som har til hensikt å anskaffe en vare eller tjeneste, kan være anskaffelsesmyndighet. Denne rollen medfører å ha sikkerhetsmessig ansvar for leverandøren, noe som innebærer tilsynsaktiviteter. Dette er rådgivning, veiledning, kontroll og oppfølging for å etablere og vedlikeholde en tilfredsstillende forebyggende sikkerhetstjeneste hos leverandøren.
Hvem beslutter hvilken sikkerhetsgradering en anskaffelse skal ha? Anskaffelsesmyndigheten har ansvar for dette med mindre det er en annen virksomhet som er bruker av varen eller tjenesten. Da er det denne som har ansvaret. Dersom det er flere brukere har anskaffelsesmyndigheten ansvaret for å utarbeide graderingsspesifikasjon for områder som er felles for brukerne.
Hvordan foretas utvelgelse av leverandører? Det er anskaffelsesmyndigheten som velger ut leverandør i henhold til alminnelige bestemmelser som gjelder for forvaltningens anskaffelsesvirksomhet
Hva kreves for å kunne utlevere sikkerhetsgradert informasjon til en leverandør? Anskaffelsesmyndighet skal ved alle anbudsinnbydelser begrense spredning av skjermingsverdig informasjon til det som er høyst nødvendig. Sikkerhetsgradert informasjon kan ikke under noen omstendighet utleveres uten gyldig sikkerhetsavtale mellom anskaffelsesmyndighet og leverandør.
Hva er en sikkerhetsavtale? Sikkerhetsavtalen formaliserer sikkerhetsmessige aspekter i forbindelse med anskaffelsen. Forskrift om sikkerhetsgraderte anskaffelser regulerer hva som minimum skal være med i en sikkerhetsavtale. Sikkerhetsavtale skal utarbeides av anskaffelsesmyndigheten. Sikkerhetsavtale skal inngås på nivå BEGRENSET og høyere.
Når benyttes og hvem trenger en leverandørklarering? Leverandørklarering må foreligge for anskaffelser på KONFIDENSIELT nivå og høyere.
Hva er gyldigheten for en leverandørklarering? En leverandørklarering gis for 5 år av gangen. Leverandørklarering kan opphøre dersom leverandøren ikke lenger vurderes til å være sikkerhetsmessig skikket.
Hvordan gjennomføres klarering av personell hos leverandør? Leverandører som innehar en leverandørklarering skal fremme anmodning om sikkerhetsklarering til anskaffelsesmyndigheten. Leverandørens daglige leder og styremedlemmer samt personell som vil få tilgang på sikkerhetsgradert informasjon skal sikkerhetsklareres. Dersom det ikke er nødvendig eller mulig å gi styremedlemmer sikkerhetsklarering skal erklæring om fraskrivelse av innsynsrett innhentes.

Vedlegg 3 Kontrollskjema

Kontrollskjemaet kan benyttes ved planlegging og gjennomføring av sikkerhetsinspeksjon hos leverandør av sikkerhetsgraderte anskaffelser i forbindelse med førstegangs- og periodiske inspeksjoner. Sjekklisten kan også benyttes i forbindelse med virksomhetens internkontroll.

Post	Gjøremål/kontrollaktivitet	Graderingsnivå	
		BEGRENSET	KONFIDENSIELT
1	FORBEREDELSER TIL INSPEKSJON		
1.1	**Historikk** Gjennomgang av rapporter fra tidligere inspeksjoner og tilsyn. Identifiser gjentakende avvik og observasjoner.		
1.2	**Grunnlagsdokument sikkerhet** Gjennomgang av virksomhetens GDS med fokus på at den ivaretar de grunnleggende forutsetninger for virksomhetens håndtering av skjermingsverdig informasjon iht forskrift om sikkerhetsadministrasjon § 3-3 slik at det dekker området sikkerhetsgraderte anskaffelser.		
1.3	**Anskaffelser** Gjennomgang av pågående leveranser og eventuell nye det søkes leverandørklarering for.		
1.4	**Graderingsspesifikasjon** Gjennomgang av verdivurdering og graderingsspesifikasjon		
1.5	**Sikkerhetsavtale** Gjennomgang av eksisterende og ny sikkerhetsavtale. Identifiser spesielle forhold som skal kontrolleres		
1.6	**Andre forhold** Identifiser spesielle sikkerhetskrav til anskaffelsene herunder MOU/PSI.		
1.7	**Administrative forhold** Gjør avtale med leverandør om tid, sted og deltagere samt spesielle forhold ifm adgang til objektet.		

2	GJENNOMFØRING AV INSPEKSJON – TEMA SIKKERHETSSTYRING		
2.1	**Sikkerhetsklarering og autorisasjon** Gjennomgang av autorisasjonslister. Vurder omfang og nivå på sikkerhetsklarert personell er iht forventet behov ifm leveransen. Kontroller eventuelt fraskrivelse av innsynsrett. Gjennomgang av rutiner for autorisasjon. Gjennomgang av saksomslag. Stikkprøver om saksomslagene er riktig utfylt. Kontroll av journal, oppbevaring og tilgang.		
2.2	**Selskapsstruktur** Identifiser de deler av selskapet / konsernet som omfattes av anskaffelsen og eventuell bruk av datterselskaper.		
3	GJENNOMFØRING AV INSPEKSJON – TEMA ANSKAFFELSER		
3.1	**Grunnlagsdokument sikkerhet** Gjennomgang av GDS generelt og rutiner spesielt.		
3.2	**Leverandører** Gjennomgang av leverandører og underleverandører for eventuell leverandørklarering.		
3.3	**Sikkerhetsavtaler** Gjennomgang av eksisterende og fremtidige sikkerhetsavtaler. Gjennomgang av eventuelt øvrig sikkerhetsdokumentasjon.		
3.4	**Objektsikkerhet** Fysisk og elektronisk sikring av lokaler for anskaffelsen. Soneinndeling og sikringstiltak.		
3.5	**Informasjonssystemer** Informasjonssystemer som skal benyttes i anskaffelsen. Logiske sikringstiltak.		
3.6	**Organisasjon** Organisering av anskaffelsen. Dokumenterte og tydelige ansvarsforhold. Organisatoriske sikringstiltak. Kommunikasjon av sikkerhetsgradert informasjon internt og eksternt.		
3.7	**Oppbevaring og bruk, journalføring av dokumentasjon** Rutiner for oppbevaring, bruk, journalføring, tilbakelevering og nødmakulering av dokumentasjon.		
3.8	**Utenlandske oppdragsgivere og leverandører** Gjennomgang av spesielle forhold ved bruk av utenlandske		

	leverandører eller ved utenlandske oppdragsgivere.		
3.9	**Autorisasjon** Ved behov gjennomføre autorisasjon av daglig leder.		
4	ETTERARBEID OG AVSLUTNING		
4.1	**Rapportering** Inspeksjonsrapport til leverandør. Eventuelt rapport til NSM dersom andre er bemyndiget til å gjennomføre inspeksjonen		
4.2	**Godkjenning av informasjonssystemer** Dersom det kreves godkjenning av informasjonssystemer koordineres dette med den instans som har myndighet til å godkjenne systemet. (NSM/FLO).		
4.3	**Lukking av avvik** Leverandørklarering gis når avvik er lukket. Alle avvik må derfor være relevant for anskaffelsen		
4.4	**Ny inspeksjon** Dato for eventuell ny inspeksjon		

Vedlegg 4 Skjema til bruk i sikkerhetsgraderte anskaffelser

Skjemaene kan lastes ned fra https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger.

Vedlegg A: Kontrollskjema for sikkerhetsgraderte anskaffelser.

Vedlegg B: Leverandørblankett

Vedlegg C: Graderingsspesifikasjon.

Vedlegg D: Egenopplysninger i forbindelse med leverandørklareringer.

Vedlegg E1: Fraskrivelse av innsynsrett (norsk).

Vedlegg E2: Fraskrivelse av innsynsrett (engelsk).

Vedlegg F: Leverandørvedlegg til personopplysningsblanketten.

Vedlegg G: Rapport etter sikkerhetsinspeksjon.

Vedlegg H1: Sikkerhetsavtale på nivå BEGRENSET.

Vedlegg H2: Sikkerhetsavtale på nivå KONFIDENSIELT eller høyere.

Vedlegg H3: Security Clauses

Vedlegg I: Request for Visit