



Vedlegg 8 A

Sikkerhet

1 Autorisasjon og eventuell sikkerhetsklarering av leverandørens personell

For avrop på rammeavtalen som innebærer at leverandørens personell skal få tilgang til sikkerhetsgradert informasjon eller skjermingsverdig objekt eller infrastruktur, vil det stilles krav til at vedkommende skal autoriseres. Dersom vedkommende skal ha tilgang til informasjon gradert KONFIDENSIELT eller skjermingsverdig objekt eller infrastruktur skal vedkommende i tillegg inneha gyldig sikkerhetsklarering.

Leverandøren skal til enhver tid ha et tilstrekkelig antall personer med gyldig sikkerhetsklarering slik at ethvert oppdrag i henhold til rammeavtalen kan løses uten forsinkelser og med den kvalitet som beskrevet.

For å hindre forsinkelser kreves det at noe leverandørpersonell sikkerhetsklareres etter inngåelse av rammeavtale, men før inngåelse av avrop. Det personellet som Leverandøren ønsker å benytte under utførelse av oppdragene må ha et reelt tjenstlig behov. Behovet må skriftlig begrunnes for den enkelte.

For denne rammeavtalen vil det være behov for å sikkerhetsklarere **5** personer for konkurranseområdet kunngjøringen gjelder. Klareringsnivået er HEMMELIG. og NATO SECRET.

Etter at rammeavtalen er inngått og avtalen er virksom vil behov for å sikkerhetsklarere personell variere ut fra omfang av bruken av rammeavtalen og det tjenstlige behovet.

Krav til beskyttelse av skjermingsverdig informasjon (ugradert eller sikkerhetsgradert), skjermingsverdige informasjonssystemer og skjermingsverdige objekter og infrastruktur er gitt i vedlegg 8 B.

1.1.1 Personopplysningsblankett (POB)

Leverandøren skal snarest etter at mottak av informasjon om hvordan personopplysningsblanketter skal fylles ut ha levert inn blanketter for det antallet som følger av pkt. 1.1, 4. avsnitt.

Med «levert», menes levering av utfylte personopplysningsblanketter som kan sendes inn til Forsvarets sikkerhetsavdeling (FSA) fra Sentral Anmodende Myndighet i Forsvarsbygg.

Leverandørens priser inkludere tidsbruk og eventuelle kostnader forbundet tidsbruk i forbindelse med utfylling av POB. Dersom det kreves at leverandørens personell må reise til annet sted enn kontraktens opplistede geografiske dekningsområde for gjennomføring av sikkerhetssamtale, godtgjøres reisetid og reisekostnader i henhold til kontraktens bestemmelser for slik godtgjørelse.

1.2 Autorisasjon

For alle avrop må det påregnes autorisasjon av personell. En autorisasjon er en samtale som skjer som regel etter at en person er sikkerhetsklarert.

Hovedregelen er at det skal foreligge sikkerhetsklarering før autorisasjon. For noen avrop kan det være tilstrekkelig at man bare autoriseres, og ikke sikkerhetsklareres, men dette er unntakene. For noen lokasjoner er det tilstrekkelig at man autoriseres en gang for lokasjonen/leiren, men det kan også være nødvendig med ytterligere autorisasjon for det enkelt avrop/bygg. Dette vil avhenge av det konkrete avropet.

Leverandøren må dekke utgifter til å oppfylle krav, som autorisasjon som følger av sikkerhetsloven med forskrifter, hvis ikke noe annet følger av avtalen, sikkerhetsavtalen eller forskrift (se forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 (klareringsforskriften) § 31).

Leverandøren kan legge til grunn at tiden til autorisasjonssamtaler ikke vil overstige en time per person per autorisasjon. Dersom det kreves at leverandørens personell må reise til annet sted enn kontraktens opplistede geografiske dekningsområde for gjennomføring av autorisasjonssamtale, godgjøres reisetid og reisekostnader i henhold til kontraktens bestemmelser for slik godtgjørelse.

2 Sikkerhetsavtaler

Det skal inngås sikkerhetsavtaler med leverandøren der dennes personell skal gis tilgang til sikkerhetsgradert informasjon, skjermingsverdige informasjonssystemer, skjermingsverdige objekter eller skjermingsverdig infrastruktur.

For denne rammeavtalen er det krav til inngåelse av sikkerhetsavtale dersom det enkelt avrop der avropet er en sikkerhetsgradert anskaffelse.

Sikkerhetsavtalen termineres av oppdragsgiver når avropet er avsluttet og leverandøren har tilbakelevert all skjermingsverdig informasjon. En eventuell service- reklamasjons- og garantitid inngår i kontraktsforholdet, og kan medføre at sikkerhetsavtale må opprettholdes etter at overlevering er skjedd.

Vedlegg 8 B

Orientering til leverandører om krav til håndtering og beskyttelse av sikkerhetsgradert informasjon i leverandørens egne lokaler

Innhold

Innhold.....	1
1. Innledning.....	2
1.1. Formål.....	2
1.2. Definisjoner.....	2
1.3. Sikkerhet i anskaffelser.....	2
1.4. Hjemmel.....	3
1.4.1. Sikkerhetsloven med forskrifter.....	3
1.4.2. Forholdet til regelverket om offentlige anskaffelser.....	3
1.5. Generelle krav til forebyggende sikkerhetsarbeid.....	3
1.5.1. Styringssystem for sikkerhet.....	3
1.5.2. Leverandørens ansvar.....	3
1.5.3. Krav om forsvarlig sikkerhetsnivå.....	3
1.5.4. Utgifter til oppfyllelse av sikkerhetskrav.....	4
1.5.5. Brudd på sikkerhetskrav.....	4
2. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå.....	4
2.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET.....	4
2.2. Inngåelse av sikkerhetsavtale på BEGRENSET nivå.....	4
2.2.1. Autorisasjon.....	5
2.2.2. Autorisasjon av utenlandsk statsborger.....	5
2.2.3. Godkjenning av skjermingsverdig informasjonssystem.....	6
2.2.4. Unntak fra krav om sikkerhetsavtale.....	6
2.2.5. Brudd på sikkerhetskrav.....	6
3. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå.....	7
3.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT.....	7
3.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT.....	7
3.1.2. Godkjenning av skjermingsverdig informasjonssystem.....	7
3.1.3. Leverandørklarering.....	7
3.1.4. Sikkerhetsklarering og autorisasjon av leverandørpersonell.....	7
3.1.5. Sikkerhetsklarering og autorisasjon av leverandørpersonell med utenlandsk statsborgerskap.....	8
3.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå.....	8
3.2.1. Brudd på sikkerhetskrav.....	8

1. Innledning

1.1. Formål

Formålet med denne orienteringen er å bidra til å gjøre leverandører av varer og tjenester til Forsvarsbygg (oppdragsgiver) oppmerksom på sikkerhetskrav som skal oppbevare, behandle eller tilvirke sikkerhetsgradert informasjon i sine egne lokaler.

1.2. Definisjoner

Sikkerhetsgradert anskaffelse: anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til sikkerhetsgradert informasjon eller informasjonssystemer som behandler slik informasjon (skjermingsverdig informasjonssystem), eller kan få tilgang til skjermingsverdig objekt eller skjermingsverdig infrastruktur.

Forebyggende sikkerhetstjeneste: planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende tiltak mot sikkerhetstruende virksomhet og følger av slik virksomhet.

Sikkerhetstruende virksomhet: tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser, eksempelvis forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandling, samt medvirkning til slik virksomhet.

Sikkerhetsgradert informasjon: informasjon som er merket med sikkerhetsgrad (BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG).

Skjermingsverdig objekt og skjermingsverdig infrastruktur: eiendom og infrastruktur som er utpekt og klassifisert av et departement eller Nasjonal sikkerhetsmyndighet (NSM), fordi det kan skade grunnleggende nasjonale funksjoner om objektene eller infrastrukturen får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettstridig overtakelse.

Nasjonale sikkerhetsinteresser: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

- a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet
- b) forsvar og beredskap
- c) forholdet til andre stater og internasjonale organisasjoner
- d) økonomisk stabilitet
- e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

Grunnleggende nasjonale funksjoner: tjenester, produksjon, og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Styringssystem for sikkerhet: styringssystem som utgjør rammen for hvordan leverandøren oppfyller kravene til forebyggende sikkerhet. Styringssystemet for sikkerhet skal sikre at sikkerhetsarbeidet planlegges, gjennomføres og kontinuerlig utvikles på en systematisk måte og helhetlig måte.

1.3. Sikkerhet i anskaffelser

Ved anskaffelse av varer og tjenester skal oppdragsgiver ta stilling til hva leverandører og deres personell (omfatter også tilbydere, underleverandører) kan få tilgang til av sikkerhetsgradert informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur (skjermingsverdige verdier) i de ulike fasene av en anskaffelse.

I konkurransegrunnlaget kan det bli stilt krav om at leverandøren må være i stand til å til å håndtere og beskytte sikkerhetsgradert informasjon i sine egne lokaler. I den forbindelse vil oppdragsgiver gi råd og veiledning om hvordan den forebyggende sikkerhetstjenesten skal praktiseres for å gi et forsvarlig sikkerhetsnivå.

1.4. Hjemmel

1.4.1. Sikkerhetsloven med forskrifter

Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven, heretter forkortet sl.) gjelder for statlige, fylkeskommunale og kommunale organer, samt leverandører av varer og tjenester i forbindelse med anskaffelser etter loven.

Sentrale forskrifter som er hjemlet i sikkerhetsloven:

- Forskrift om virksomheters arbeid med forebyggende sikkerhet av 20. desember 2018 nr. 2053 (virksomhetsikkerhetsforskriften, heretter forkortet vsf.)
- Forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 nr. 2054 (klareringsforskriften, heretter forkortet kf)

1.4.2. Forholdet til regelverket om offentlige anskaffelser

Reglene om sikkerhetsgraderte anskaffelser kommer i tillegg til reglene som gjelder for offentlige anskaffelser (anskaffelsesloven) med tilhørende forskrifter.

1.5. Generelle krav til forebyggende sikkerhetsarbeid

1.5.1. Styringssystem for sikkerhet

Leverandører som omfattes av sikkerhetsloven og skal oppbevare, behandle eller tilvirke sikkerhetsgradert informasjon i sine egne lokaler, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at leverandøren oppfyller kravene gitt i eller med hjemmel i sikkerhetsloven.

Under utførelse av anskaffelsen på en av Forsvarsbyggs eller Forsvarets lokasjoner, er oppdragsgivers styringssystem for sikkerhet gjeldende.

1.5.2. Leverandørens ansvar

Sikkerhetskravene som gjøres gjeldende for leverandøren vil avhenge av hva leverandøren og dennes personell får tilgang til, og hvordan denne tilgangen gis.

Leverandørens daglige leder har ansvaret for det forebyggende sikkerhetsarbeidet innen sitt ansvars- og myndighetsområde, herunder underlagte virksomheter.

1.5.3. Krav om forsvarlig sikkerhetsnivå

Det stilles funksjonelle krav til håndtering av risiko knyttet til sikkerhetsgradert informasjon. Funksjonelle krav innebærer at det stilles krav om hva sikkerhetstiltakene i virksomhetene skal oppnå, ikke hvordan kravene oppnås. Det er derfor, med visse unntak, ikke avgjørende hvilke sikkerhetstiltak som velges, så lenge de valgte tiltakene gjør at det oppnås et forsvarlig sikkerhetsnivå. Det legges således opp til at leverandøren kan velge å kombinere fysiske, elektroniske, menneskelige og organisatoriske tiltak, så lenge virksomheten har et forsvarlig sikkerhetsnivå.

Leverandøren skal identifisere, analysere og evaluere risiko for at kravet om forsvarlig sikkerhetsnivået ikke kan oppfylles. På bakgrunn av risikovurderingen skal leverandøren gjennomføre de forebyggende sikkerhetstiltakene som er nødvendig for å oppnå et forsvarlig sikkerhetsnivå.

Leverandøren skal dokumentere at han på en tilfredsstillende måte både har vurdert og håndtert risiko og hvilke sikkerhetstiltak som er etablert.

NSM har publisert veiledere som gir anbefalinger om hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket. NSM har i tillegg publisert 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, se www.nsm.no.

Det kan være behov for veiledere som er sikkerhetsgradert eller er unntatt offentlighet. Forsvarsbygg vil fremskaffe slike veiledere ved behov. Dette er spesielt aktuelt på KONFIDENSIELT nivå.

1.5.4. Utgifter til oppfyllelse av sikkerhetskrav

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av sikkerhetsloven med forskrifter, hvis ikke noe annet følger av avtalen eller sikkerhetsavtalen med forskrifter (se særlig kf. § 31).

1.5.5. Brudd på sikkerhetskrav

Overtredelse av sikkerhetsbestemmelser, forsettlig eller uaktsomt, kan anses som brudd på leverandørens kontraktsforpliktelser.

2. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå

2.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET

For beskyttelse av informasjon gradert BEGRENSET, er kravet til forsvarlig sikkerhetsnivå oppfylt dersom informasjonen med enkle midler ikke kan bli kjent for uautoriserte personer, gå tapt eller endres eller gjøres utilgjengelig. Ved valg av sikkerhetstiltak skal leverandøren se behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre, jf. vsf. § 39.

2.2. Inngåelse av sikkerhetsavtale på BEGRENSET nivå

Sikkerhetsavtale mellom oppdragsgiver og leverandøren skal inngås før leverandøren kan oppbevare, behandle eller tilvirke informasjon gradert BEGRENSET i sine egne lokaler. Sikkerhetsavtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar etter sikkerhetsloven med forskrifter. Sikkerhetsavtale skal inngås for hver enkelt sikkerhetsgradert anskaffelse.

Før sikkerhetsavtalen kan inngås må leverandøren dokumentere at han oppfyller krav som sikkerhetsloven og virksomhetsikkerhetsforskriften stiller til et forsvarlig sikkerhetsnivå.

Følgende dokumenter må utarbeides av leverandøren og sendes til oppdragsgiver:

- Beskrivelse av virksomhetens styringssystem for sikkerhet og bekreftelse på at styringssystemet er implementert, jf. sl. § 4.1 og vsf. § 3.
- Styringsdokument for det forebyggende sikkerhetsarbeidet, jf. vsf. § 4.
- Sikkerhetsmål, jf. vsf. § 5.
- Beskrivelse av roller og ansvar i den lokale sikkerhetsorganisasjonen, jf. vsf. § 6.
- Bekreftelse på at personellet i den lokale sikkerhetsorganisasjonen og personellet som skal håndtere sikkerhetsgradert informasjon i forbindelse med anskaffelsen har tilstrekkelig kompetanse om forebyggende sikkerhetstjeneste, jf. sl. § 4-1 andre ledd og vsf. § 7.
- Risikovurdering og beskrivelse av hvordan risiko håndteres, jf. sl. §§ 4-2 og 4-4, samt vsf. §§ 12 og 13.
- Beskrivelse av lokalt etablerte sikkerhetstiltak (grunnsikringstiltak) og planlagte påbyggingstiltak samt tegning/skisse av lokalene hvor sikkerhetsgradert informasjon skal oppbevares og behandles, jf. sl. § 4-4, samt vsf. §§ 14 og 15. Ved etablering av fysiske sikkerhetstiltak oppfordres leverandøren til å følge Nasjonalt kompetansesenter for sikring av bygg (NKS) sine anbefalte metoder for sikring av informasjon gradert BEGRENSET, jf. Sikringshåndboka – Håndbok i sikring av eiendom, bygg og anlegg mot terror, sabotasje og spionasje og annen kriminalitet (2022 eller nyere utgave).
- Beskrivelse av skjermingsverdig informasjonssystem, jf. sl. § 6-1 og vsf. kapittel 7.

Kravene i virksomhetsikkerhetsforskriften og anbefalingene i Sikringshåndboka som gjelder beskyttelse av informasjon er minimumskrav. For å styrke beskyttelsen av informasjon gradert BEGRENSET har oppdragsgiver besluttet at leverandører som har behov for å oppbevare, behandle eller tilvirke informasjon gradert BEGRENSET skal etablere følgende sikkerhetstiltak utover minimumskravene:

- Leverandøren skal etablere et rom innenfor en kontrollert sone, jf. vsf. § 39. Det skal være et fysisk skille mellom kontrollert sone og rommet. Det fysiske skillet vil normalt bestå av gulv, tak, vegger, vinduer og dør. Da det ikke skal være mulig å ta seg inn i rommet uten at det kan oppdages, skal denne avgrensningen være hel. Dette innebærer blant annet at vegger skal gå over nedsenket himling og under hevet gulv (datagulv). Der dette ikke er praktisk

gjennomførbart kan vegg over himling og under gulv erstattes med gitter eller lignende. Konstruksjonen skal være slik at bygningselementer ikke enkelt kan fjernes for så å bli satt tilbake på plass uten at det settes visuelle spor. I tillegg til den fysiske konstruksjonen skal rommet sikres mot innsyn, også fra kontrollert sone, for å oppnå en god beskyttelse mot tilgang til sikkerhetsgradert informasjon fra uautoriserte og besøkende.

- For å hindre uautorisert adgang til skal det monteres FG-godkjent lås på dør til det aktuelle rommet. Døren skal være låst og dokumenter og lagringsmedier med informasjon som er gradert BEGRENSET skal være nedlåst i en oppbevaringsenhet godkjent for KONFIDENSIELT (K-skap) når autorisert personell ikke er til stede.
- Dersom leverandøren på et senere tidspunkt vil kunne få behov for å oppbevare, behandle eller tilvirke informasjon gradert KONFIDENSIELT i sine egne lokaler, anbefales det at leverandøren før etablering av rom godkjent for BEGRENSET tar i betraktning de krav som gjelder for beskyttelse av informasjon gradert KONFIDENSIELT, se punktene 3.1 og 3.2, jf. vsf, kapittel 6 og 7 og spesielt kravene for skjerming mot Tempest.

2.2.1. Autorisasjon

Leverandørens daglige leder skal autoriseres av oppdragsgiver før sikkerhetsavtale inngås. Leverandørens daglige leder er leverandørens autorisasjonsansvarlige. Vedkommende har ansvaret for at eget personell som skal ha tilgang til informasjon gradert BEGRENSET, som oppbevares i leverandørens egne lokaler, er autorisert før tilgang gis. Det skal gjennomføres en autorisasjonssamtale før det gis autorisasjon. Krav til autorisasjonssamtalens innhold er gitt i vsf, § 68 andre ledd. NSM har publisert en Håndbok i autorisasjon og autorisasjonssamtale som kan være et nyttig hjelpemiddel.

Informasjon som inneholder personopplysninger i saker om autorisasjon, skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at det er gitt en autorisasjon eller meldinger om andre autorisasjonsavgjørelser til personen som avgjørelsen gjelder.

Den autorisasjonsansvarlige skal bestemme hvem i virksomheten som kan få tilgang til opplysninger merket PERSONKONTROLL. Slike opplysninger skal lagres atskilt fra andre opplysninger i virksomheten, og de skal bare være tilgjengelige for det utpekte personellet. Når virksomheten utveksler opplysninger merket PERSONKONTROLL, skal det gjøres på en slik måte at uvedkommende ikke får tilgang til opplysningene.

Den som skal autoriseres skal signere en taushetserklæring på blankett fastsatt av NSM før det gis autorisasjon.

Leverandørens daglige leder er også ansvarlig for sikkerhetsmessig ledelse og kontroll av eget personell som er autorisert.

Det gjøres oppmerksom på at det er leverandørens risiko at autorisasjon ikke oppnås. Han har også risikoen for at autorisasjon tar uforholdsmessig lang tid, med mindre forsinkelsen skyldes forhold oppdragsgiver svarer for.

2.2.2. Autorisasjon av utenlandsk statsborger

Før en utenlandsk statsborger som ikke har klarering, kan autoriseres for informasjon gradert BEGRENSET, skal den autorisasjonsansvarlige vurdere om personens tilknytning til hjemlandet og hjemlandets sikkerhetsmessige betydning utgjør en uakseptabel risiko. Den autorisasjonsansvarlige kan be klareringsmyndigheten om en vurdering av hjemlandets sikkerhetsmessige betydning.

Dersom en utenlandsk statsborger kommer fra en stat som Politiets sikkerhetstjeneste (PST) mener utgjør en høy sikkerhetsrisiko for Norge, se PSTs årlige nasjonale trusselvurdering, må den autorisasjonsansvarlige innhente samtykke fra klareringsmyndigheten (Forsvarets sikkerhetsavdeling (FSA)) før den utenlandske statsborgeren kan autoriseres for BEGRENSET. Dette kravet gjelder også for personer som har dobbelt statsborgerskap (hvorav det ene er norsk), er statsløse eller har uavklart statsborgerskap.

2.2.3. Godkjenning av skjermingsverdig informasjonssystem

Ved behov kan det etableres et skjermingsverdig informasjonssystem hos leverandøren for å behandle sikkerhetsgradert informasjon. For å kunne behandle sikkerhetsgradert informasjon på nivå BEGRENSET hos leverandøren, må leverandøren etablere og drifte et skjermingsverdig informasjonssystem. Informasjonssystemet skal godkjennes i henhold til vsf §§ 50-53.

I vsf § 49 stilles det funksjonelle krav for skjermingsverdige informasjonssystemer. Ved å følge NSMs veiledere for godkjenning av informasjonssystemer anses kravene i vsf § 49 som ivaretatt.

Leverandøren må ha en sikkerhetsavtale for angjeldende anskaffelse før skjermingsverdig informasjonssystem kan installeres og tas i bruk.

Leverandøren må utarbeide følgende dokumentasjon i forbindelse med godkjenning av skjermingsverdige informasjonssystem:

- Brukerinstruks
- Driftsinstruks
- Beredskapsplan
- Konfigurasjonsoversikt
- Medieregister
- Risikovurdering
- Søknad om godkjenning av informasjonssystem

Oppdragsgiver har maler for hver av de ovennevnte dokumenter.

Kostnader knyttet til anskaffelse og godkjenning av skjermingsverdig informasjonssystem som skal brukes til å behandle informasjon sikkerhetsgradert BEGRENSET:

- Leverandøren skal dekke kostnaden med godkjenningen.
- Standard IT-maskinvare kan benyttes, men det skal kjøpes inn via sikre leverandørkjeder. Forsvarets godkjente produktliste (GPL) inneholder produkter fra sikre leverandørkjeder.
- Informasjonssystemet skal aldri kobles til internett eller andre nettverk. Lisensiering av programvare kan være en utfordring, fordi stadig flere programvareleverandører krever at deres programvare er tilkoblet internett slik at gyldig lisens kan registreres. Løsninger på disse utfordringer kan medføre ekstra kostnader.
- Leverandøren må sette av tid til installasjon og godkjenning av informasjonssystemet samt utarbeidelse av dokumentasjon og instruks.
- Leverandøren må sette av tid og ressurser med tilstrekkelig IT-kompetanse til løpende drift av informasjonssystemet slik at forsvarlig sikkerhetsnivå opprettholdes i hele levetiden til informasjonssystemet.
- NSMs grunnprinsipper for IKT-sikkerhet kan gi nyttig veiledning til dette arbeidet.

2.2.4. Unntak fra krav om sikkerhetsavtale

Det kreves ikke sikkerhetsavtale dersom leverandørens personell bare skal gis tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller infrastruktur under oppsyn av en representant for oppdragsgiver, jf. vsf § 81. I NSMs Veileder i anskaffelser etter sikkerhetsloven redegjøres det for hva som menes med «oppsyn».

For å oppnå et forsvarlig sikkerhetsnivå under anskaffelsen kan oppdragsgiver, med bakgrunn i risikovurdering, beslutte at sikkerhetsavtale skal inngås selv om kravet til oppsyn er oppfylt.

2.2.5. Brudd på sikkerhetskrav

Dersom leverandøren ikke retter brudd på kravene fastsatt i eller med hjemmel i sikkerhetsloven innen en fastsatt frist, kan oppdragsgiver si opp sikkerhetsavtalen. Er et brudd vesentlig, kan oppdragsgiver si opp sikkerhetsavtalen uten at det settes en frist.

3. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå

3.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT

Vsf. kapittel 6 fastsetter krav til beskyttelse av informasjon gradert KONFIDENSIELT.

Kravene som gjelder på BEGRENSET nivå, vil også gjelde for KONFIDENSIELT nivå.

3.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT

For å beskytte skjermingsverdig informasjonssystem og informasjon gradert KONFIDENSIELT eller høyere, skal det etableres en kontrollert og beskyttet sone. Dersom leverandøren har behov for et eget rom med direkte tilgang til informasjon gradert KONFIDENSIELT, skal det etableres en sperret sone, jf. vsf. kapittel 6, NSMs Veileder i fysisk sikkerhet og Sikringshåndboka.

3.1.2. Godkjenning av skjermingsverdig informasjonssystem

Ved behov skal leverandøren etablere et skjermingsverdig informasjonssystem for behandling av informasjon gradert KONFIDENSIELT. Informasjonssystemet skal godkjennes i henhold til vsf. §§ 50-53.

Elektronisk utstyr avgir stråling som medfører at informasjon kan avleses på avstand uten at noen oppdager det. I vsf. §34 er det krav om at uautoriserte personer ikke kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, uten at virksomheten oppdager det. Tempestrisikovurdering må derfor utarbeides i tillegg til dokumentasjonen som er aktuell for skjermingsverdig informasjonssystem på BEGRENSET nivå. Oppdragsgiver kan fremskaffe mal for Tempestrisikovurdering.

En leverandør til en sikkerhetsgradert anskaffelse skal ha en leverandørklarering når det er nødvendig for å oppnå et forsvarlig sikkerhetsnivå under anskaffelsen. Leverandørklarering gis av NSM.

Kostnader knyttet til anskaffelse og godkjenning av skjermingsverdig informasjonssystem som skal brukes til å behandle informasjon sikkerhetsgradert KONFIDENSIELT:

- Virksomheten skal dekke kostnaden med godkjenningen.
- Tempestrisikovurdering avgjør om Tempestgodkjent IT-maskinvare må benyttes. Forsvarsbyggs leverandører må normalt benytte Tempestgodkjent maskinvare i informasjonssystemer på KONFIDENSIELT nivå. Prisen på Tempestgodkjent maskinvare kan være 30-50% høyere enn standard maskinvare og leveringstiden kan være flere uker.
- Informasjonssystemets avstand til områder som er utenfor leverandørens kontroll har betydning for hvilke Tempesttiltak som er nødvendig, og dermed også kostnader. Bestemmelser om avstander og tiltak er sikkerhetsgradert, og informasjon kan bare utleveres til leverandøren ved behov.
- Leverandøren må sette av tid til etablering av informasjonssystemet samt utarbeidelse av dokumentasjon og instruks. Det er flere krav på KONFIDENSIELT nivå og dette kan medføre flere instruks og dokumentasjon.

3.1.3. Leverandørklarering

Leverandør som skal oppbevare, behandle eller tilvirke informasjon gradert KONFIDENSIELT i egne lokaler, skal ha leverandørklarering gitt av NSM før sikkerhetsavtale kan inngås med oppdragsgiver.

Før leverandørklarering kan gis skal NSM kontrollere at leverandøren oppfyller kravene i sikkerhetsloven, virksomhetsikkerhetsforskriften og klareringsforskriften.

3.1.4. Sikkerhetsklarering og autorisasjon av leverandørpersonell

Leverandørpersonell som har behov for tilgang til informasjon som er sikkerhetsgradert KONFIDENSIELT eller høyere skal ha gyldig sikkerhetsklarering for angjeldende sikkerhetsgrad. Kravet om sikkerhetsklarering gjelder også for leverandørpersonell som har behov for tilgang til skjermingsverdig objekt eller skjermingsverdig infrastruktur.

Før leverandørklarering kan gis skal leverandørens daglige leder og alle styremedlemmer inkludert varamedlemmer sikkerhetsklareres for det samme nivå som det er anmodet om leverandørklarering for. Dersom leverandørens daglige leder eller et styremedlem ikke kan sikkerhetsklareres, må vedkommende skriftlig gi avkall på innsyn i den sikkerhetsgraderte anskaffelsen.

Informasjon som inneholder personopplysninger i saker om autorisasjon, personkontroll eller sikkerhetsklarering, skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at det er gitt en autorisasjon eller sikkerhetsklarering eller meldinger om andre autorisasjons- eller sikkerhetsklaringsavgjørelser til personen som avgjørelsen gjelder. For tilgang til opplysninger merket PERSONKONTROLL, se punkt 2.2.1.

Leverandørens daglige leder skal autoriseres av oppdragsgiver før sikkerhetsgradert informasjon utleveres til eller tilvirkes i leverandørens egne lokaler.

Leverandørens daglige leder skal sørge for at eget personell, med behov for tilgang til informasjon gradert KONFIDENSIELT som er i leverandørens besittelse, har gyldig sikkerhetsklarering før autorisasjon gis.

Det gjøres oppmerksom på at det er leverandørens risiko at autorisasjon eller sikkerhetsklarering ikke oppnås.

3.1.5. Sikkerhetsklarering og autorisasjon av leverandørpersonell med utenlandsk statsborgerskap

En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering bli sikkerhetsklarert, dersom det ikke er rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. I tillegg til forholdene som er nevnt i sikkerhetsloven § 8-4 skal det i vurderingen legges vekt på hjemlandets sikkerhetsmessige betydning, personens tilknytning til hjemlandet og tilknytningen til Norge. Utfallet av slike søknader er usikkert, og i alle tilfeller må det påregnes vesentlig lengre saksbehandlingstid enn for norske statsborgere.

3.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå

Sikkerhetsavtale mellom oppdragsgiver og leverandøren skal inngås før leverandøren kan oppbevare, behandle eller tilvirke informasjon gradert KONFIDENSIELT i sine egne lokaler.

Før sikkerhetsavtalen kan inngås må leverandøren dokumentere at han oppfyller krav som sikkerhetsloven og virksomhetsikkerhetsforskriften stiller til et forsvarlig sikkerhetsnivå for sikkerhetsgrad KONFIDENSIELT.

3.2.1. Brudd på sikkerhetskrav

Dersom leverandøren ikke retter brudd på kravene fastsatt i eller med hjemmel i sikkerhetsloven innen en fastsatt frist, kan leverandørklarering kalles tilbake av NSM. Er et brudd vesentlig, kan NSM tilbakekalle leverandørklareringen uten at det settes en frist. Dersom leverandørklareringen kalles tilbake, vil sikkerhetsavtalen sies opp.