FORSVARSBYGG

Vedlegg 5 – Orientering til leverandører om krav til håndtering og beskyttelse av skjermingsverdig informasjon i forbindelse med anskaffelser

Innholdsfortegnelse

1. Innledning 2
   1.1. Formål 2
   1.2. Definisjoner 2
   1.3. Sikkerhet i anskaffelser 2
   1.4. Hjemmel 3
      1.4.1. 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 3
      1.5.5. Brudd på sikkerhetskrav 3
2. Anskaffelser på skjermingsverdig ugradert nivå 4
   2.1. Veiledere 4
3. Sikkerhetsgraderte anskaffelser 4
4. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå 4
   4.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET 4
   4.2. Inngåelse av sikkerhetsavtale på BEGRENSET nivå 4
      4.2.1. Autorisasjon 5
      4.2.2. Autorisasjon av utenlandsk statsborger 5
      4.2.3. Godkjenning av skjermingsverdige informasjonssystem 5
      4.2.4. Unntak fra krav om sikkerhetsavtale 6
      4.2.5. Innholdet i sikkerhetsavtalen 6
      4.2.6. Brudd på sikkerhetskrav 7
      4.2.7. Ytterligere sikkerhetskrav 7
      4.2.8. NSMs veiledere og håndbøker 7
5. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå eller høyere 7
   5.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT eller høyere 7
      5.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere 7
      5.1.2. Godkjenning av skjermingsverdig informasjonssystem 8
      5.1.3 Leverandørklarering 8
      5.1.4 Sikkerhetsklarering og autorisasjon av leverandørpersonell 8
   5.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå eller høyere 9
      5.2.1. Brudd på sikkerhetskrav 9
      5.2.2. Ytterligere krav 9
      5.2.3. NSMs veiledere og håndbøker 9

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 kan gjøres gjeldende i anskaffelsesprosessen.

1.2. Definisjoner

Sikkerhetsgradert anskaffelse: anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til skjermingsverdig informasjon eller informasjonssystemer som behandler slik informasjon, 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 terrorhandlinger, samt medvirkning til slik virksomhet.

Skjermingsverdig informasjon: Samlebetegnelse som benyttes om all informasjon som skal beskyttes etter sikkerhetsloven. Informasjonen kan være sikkerhetsgradert eller ugradert.

Ugradert skjermingsverdig informasjon: informasjon som har betydning for grunnleggende nasjonale funksjoner, men som ikke er sikkerhetsgradert. Informasjonen er skjermingsverdig ut ifra en integritets- og tilgjengelighetsvurdering, dvs. at den kan skade nasjonale sikkerhetsinteresser dersom den går tapt eller blir endret (integritet), eller gjort utilgjengelig (tilgjengelighet).

Sikkerhetsgradert skjermingsverdig informasjon: informasjon som er merket med sikkerhetsgrad (BEGRENSET, KONFIDENSIELT, HEMMELIG eller STRENGT HEMMELIG). Informasjonen er skjermingsverdig ut ifra en integritets-, tilgjengelighets- og konfidensialitetsvurdering, dvs. den kan skade nasjonale sikkerhetsinteresser om den går tapt eller blir endret (integritet), gjort utilgjengelig (tilgjengelighet) eller blir kjent for uvedkommende (konfidensialitet).

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.

Skjermingsverdig informasjonssystem: informasjonssystem som behandler skjermingsverdig informasjon, eller som har avgjørende betydning for grunnleggende nasjonale funksjoner.

Skjermingsverdig verdi: skjermingsverdig objekt, infrastruktur, informasjon eller informasjonssystem.

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 (omfatter også tilbydere og underleverandører) kan få tilgang til av skjermingsverdig informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur 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 skjermingsverdig informasjon i sine egne lokaler, eller oppfylle krav som stilles for tilgang til

skjermingsverdig informasjon, skjermingsverdig objekt eller skjermingsverdig infrastruktur hos oppdragsgiver. I den forbindelse vil oppdragsgiver gi råd og veiledning om forebyggende sikkerhetstjeneste.

1.4. Hjemmel

Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven) 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)
- Forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 nr. 2054 (klareringsforskriften)

1.4.1. 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.

1.5.2. Leverandørens ansvar

Leverandøren eller personell fra leverandøren skal oppfylle de samme krav til sikkerhet som gjelder for oppdragsgiver. Kravene til leverandøren vil avhenge av hva leverandøren får tilgang til, og hvordan denne tilgangen gis.

Leverandørens leder har ansvaret for det forebyggende sikkerhetsarbeidet innen sitt ansvars- og myndighetsområde, herunder underlagte virksomheter. Det kreves at sikkerhetsarbeidet utøves på en proaktiv og systematisk måte.

1.5.3. Krav om forsvarlig sikkerhetsnivå

Det stilles funksjonelle krav til håndtering av risiko knyttet til skjermingsverdig 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.

1.5.4. Utgifter til oppfyllelse av sikkerhetskrav

Leverandøren må selv dekke utgifter til å oppfylle krav som følger av lovens bestemmelser, hvis ikke noe annet følger av avtalen, sikkerhetsavtalen med Forsvarsbygg (oppdragsgiver) eller forskrifter (se sikkerhetsloven § 9-2 tredje ledd og klareringsforskriften § 31).

1.5.5. Brudd på sikkerhetskrav

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

2. Anskaffelser på skjermingsverdig ugradert nivå

Ved håndtering av risiko knyttet til skjermingsverdig ugradert informasjon skal det etableres forebyggende sikkerhetstiltak som et minimum sørger for at informasjonen ikke kan gå tapt, endres eller gjøres utilgjengelig med enkle midler. Ved valg av sikkerhetstiltak skal leverandøren se behovet for å beskytte informasjonens integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre.

2.1. Veiledere

For virksomheter som skal ha tilgang til skjermingsverdig ugradert informasjon vil NSMs Håndbok i beskyttelse av skjermingsverdig ugradert informasjon være relevant å benytte i det forebyggende sikkerhetsarbeidet, se https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/

3. Sikkerhetsgraderte anskaffelser

I sikkerhetsloven kapittel 9 og virksomhetsikkerhetsforskriften kapittel 13 stilles det særskilte krav til oppdragsgiver og leverandører i forbindelse med sikkerhetsgraderte anskaffelser.

Skal leverandøren oppbevare, behandle eller tilvirke sikkerhetsgradert informasjon i sine egne lokaler, eller gis tilgang til skjermingsverdig objekt eller infrastruktur fra sine egne lokaler, må leverandøren oppfylle de krav som sikkerhetsloven med forskrifter stiller til virksomheter med tilsvarende mulighet til å råde over samme informasjon, objekt eller infrastruktur. Det understrekes at underleverandører med samme tilgang også må oppfylle kravene i sikkerhetsloven med forskrifter.

4. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå

4.1. 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. Dette kravet kommer i tillegg til ovennevnte krav som gjelder for beskyttelse av skjermingsverdig ugradert informasjon. Ved valg av sikkerhetstiltak skal leverandøren se behovet for å beskytte informasjonens konfidensialitet, integritet og tilgjengelighet i sammenheng og veie hensynene mot hverandre.

Generelle krav som gjelder vurdering og håndtering av risiko og iverksettelse av forebyggende sikkerhetstiltak, er gitt i virksomhetsikkerhetsforskriften kapittel 3 og 7.

4.2. 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. Sikkerhetsavtale skal også inngås dersom leverandøren kan gis tilgang til skjermingsverdig objekt eller infrastruktur i eller fra 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 BEGRENSET.

Følgende dokumenter må utarbeides:

- Beskrivelse av virksomhetens styringssystem for sikkerhet og bekreftelse på at styringssystemet er implementert, jf. sikkerhetsloven § 4.1 og virksomhetsikkerhetsforskriften § 3
- Styringsdokument for det forebyggende sikkerhetsarbeidet, jf. virksomhetsikkerhetsforskriften § 4
- Sikkerhetsmål, jf. virksomhetsikkerhetsforskriften § 5
- Beskrivelse av roller og ansvar i den lokale sikkerhetsorganisasjonen, jf. virksomhetsikkerhetsforskriften § 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 og kjenner til relevante sikkerhetstrusler og sikkerhetsbestemmelser, jf. sikkerhetsloven § 4-1 andre ledd og virksomhetsikkerhetsforskriften § 7
- Risikovurdering og risikohåndtering. Kopi av lokal risikovurdering må sendes inn, jf. sikkerhetsloven §§ 4-2 og 4-4 og virksomhetsikkerhetsforskriften §§ 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. sikkerhetsloven § 4-4 og virksomhetsikkerhetsforskriften §§ 14 og 15.

4.2.1. Autorisasjon

Leverandørens daglig leder skal autoriseres av oppdragsgiver før sikkerhetsavtale inngås. Daglig leder er autorisasjonsansvarlig og 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 virksomhetsikkerhetsforskriften § 68 andre ledd.

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

Informasjon som inneholder personopplysninger i saker om autorisasjon, personkontroll eller klarering, skal merkes PERSONKONTROLL. Kravet gjelder ikke meldinger om at det er gitt en autorisasjon eller klarering eller meldinger om andre autorisasjons- eller klareringsavgjørelser 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 personellets. 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.

4.2.2. 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 en klareringsmyndighet 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.

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.

4.2.3. Godkjenning av skjermingsverdige informasjonssystem

NSM er godkjenningsmyndighet for skjermingsverdige informasjonssystemer som er angitt i virksomhetsikkerhetsforskriften § 51 første og andre ledd. Skjermingsverdige informasjonssystemer som ikke er nevnt i første og andre ledd skal godkjennes av leverandøren, men oppdragsgiver skal gi tillatelse før informasjonssystemet kan tas i bruk.

Leverandøren skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. I virksomhetsikkerhetsforskriften § 49 stilles det funksjonelle krav for skjermingsverdig informasjonssystemer. Ved å følge NSMs og Forsvarsbyggs veiledere for godkjenning av informasjonssystemer anses kravene § 49 som ivaretatt.

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

Følgende dokumentasjon må utarbeides i forbindelse med godkjenning av skjermingsverdige informasjonssystemer:

- Systembeskrivelse
- Brukerinstruks
- Driftsinstruks

- Beredskapsplan
- Konfigurasjonsoversikt
- Nettverkstegning dersom lokalt lukket nettverk
- Godkjenningsskriv

Oppdragsgiver har maler for hver av de ovennevnte dokumenter.

4.2.4. 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. I «Veiledning for sikkerhetsgraderte anskaffelser» klargjøres 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.

4.2.5. Innholdet i sikkerhetsavtalen

Sikkerhetsavtalen skal tydeliggjøre og konkretisere partenes plikter og ansvar etter sikkerhetsloven med forskrifter. Sikkerhetsavtale skal inngås for hver enkelt sikkerhetsgradert anskaffelse.

I virksomhetsikkerhetsforskriften § 80 stilles det krav til innholdet i sikkerhetsavtalen.

Ved inngåelse av sikkerhetsavtale på BEGRENSET nivå vil oppdragsgiver stille krav om at leverandøren forplikter seg til å:

- vedlikeholde styringssystemet for sikkerhet
- regelmessig gjennomføre vurdering av risiko og håndtere risiko
- påse at sikkerhetstiltak (fysiske, elektroniske, menneskelige og organisatoriske) for sikkerhetsgradert informasjon og informasjonssystemer som skal behandle slik informasjon, er tilpasset aktuell risiko og oppfyller kravet til forsvarlig sikkerhetsnivå
- påse at eget personell, før de gis tilgang til sikkerhetsgradert informasjon og skjermingsverdige informasjonssystemer, har gjennomført grunnleggende opplæring i sikkerhet
- gjøre styringsdokument for sikkerhet og relevante sikkerhetsinstrukser for rutiner og prosedyrer kjent og tilgjengelig for eget personell
- oppfylle kravene for autorisasjonssamtale og autorisasjon av eget personell som har tjenstlig behov for tilgang til sikkerhetsgradert informasjon og skjermingsverdig informasjonssystem som leverandøren har i sine egne lokaler
- ivareta sikkerhetsmessig ledelse og kontroll av eget personell som er autorisert
- orientere oppdragsgiver om forhold som kan ha betydning for leverandørens leders sikkerhetsmessige skikkethet
- overholde taushetsplikten også etter at anskaffelsen er avsluttet
- løpende kontrollere at sikkerhetstiltak fungerer etter sin hensikt og at sikkerhetsbestemmelser følges
- håndtere og rapportere avvik fra sikkerhetskrav/sikkerhetsbrudd til oppdragsgiver
- påse at sikkerhetsgradert informasjon ikke utleveres til tredjepart uten at samtykke fra oppdragsgiver på forhånd foreligger
- ikke offentliggjøre deltakelse i sikkerhetsgradert anskaffelse på Internett eller i markedsføring
- orientere oppdragsgiver om forhold som er av sikkerhetsmessig betydning, herunder endring av foretaksnavn, skifte av daglig leder, flytting/ombygging av lokaler, åpning av gjeldsforhandlinger, begjæring om konkurs og annet som kan påvirke leverandørens sikkerhetsmessige skikkethet
- legge til rette for at oppdragsgiver kan gi råd og veiledning om forebyggende sikkerhetstjeneste
- legge til rette for at oppdragsgiver kan kontrollere at leverandøren oppfyller kontraktsforpliktelser knyttet til forebyggende sikkerhetstjeneste
- legge til rette for at NSM eller sektormyndighet med tilsynsansvar kan kontrollere sikkerhetstilstanden hos leverandøren

4.2.6. 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.

4.2.7. Ytterligere sikkerhetskrav

Det understrekes at ovennevnte krav ikke er uttømmende. I enkelte anskaffelser kan det, med bakgrunn i økt risiko knyttet til verdier, trusler eller sårbarheter bli stilt ytterligere krav til sikkerhet, jf. generelle krav til beskyttelse av skjermingsverdige verdier i virksomhetsikkerhetsforskriften kapittel 3.

4.2.8. NSMs veiledere og håndbøker

For leverandører med sikkerhetsavtale på BEGRENSET nivå vil NSMs veiledninger og håndbøker være relevante å benytte i det forebyggende sikkerhetsarbeidet, se https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/

5. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå eller høyere

5.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT eller høyere

Virksomhetsikkerhetsforskriften kapittel 6 fastsetter krav til beskyttelse av informasjon gradert KONFIDENSIELT eller høyere.

Kravene til sikkerhetsdokumentasjon og håndtering og beskyttelse av informasjon gradert KONFIDENSIELT eller høyere kommer i tillegg til kravene som gjelder for ugradert skjermingsverdig informasjon og informasjon gradert BEGRENSET.

5.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere

For å beskytte sikkerhetsgraderte informasjon og informasjonssystem gradert KONFIDENSIELT eller høyere, skal det etableres en kontrollert og beskyttet sone. Dersom leverandøren har et område med direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere, for eksempel arkivrom eller serverrom, skal det etableres en sperret sone rundt dette området.

En kontrollert sone skal være et tydelig avgrenset område der leverandøren skal kunne ha kontroll med personer, kjøretøy og annen aktivitet. Ved særlig høy risiko skal adgang og ferdsel kontrolleres med en fysisk avgrensning.

En beskyttet sone skal ha en fysisk avgrensning der sikkerhetstruende virksomhet skal kunne oppdages. I en beskyttet sone skal dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT eller høyere lagres i oppbevaringsenhet godkjent av NSM.

Dokumenter og lagringsmedier med informasjon som er gradert KONFIDENSIELT, skal bare oppbevares og behandles i en beskyttet sone eller sperret sone. Typiske sperrede soner vil være arkiver og dokumenthvelv, operasjonsrom, kommunikasjons- og serverrom eller lokaler der det lages sikkerhetsgraderte produkter. Dette er altså spesialrom hvor sikkerhetsgradert informasjon er åpent eller lett tilgjengelig for den som har adgang.

Personer som skal gis permanent adgang til en beskyttet eller sperret sone, skal være sikkerhetsklarert og autorisert. Det skal være kontroll med adgangen.

5.1.1.1. Balansert sikring

Verken virksomhetsikkerhetsforskriften eller NSMs veiledninger gir konkrete føringer om hvilke sikkerhetstiltak som til enhver tid er tilstrekkelig for å oppnå et forsvarlig sikkerhetsnivå. Dette må fremkomme i en risikovurdering som gjennomføres av den enkelte virksomhet.

For å redusere risiko for innbrudd kan kravet om forsvarlig sikkerhetsnivå langt på vei oppnås gjennom balansert sikring. Med balansert sikring menes at det er balanse mellom fysiske sikkerhetstiltak, deteksjonstiltak, og reaksjonstid. Balansert sikring oppnås når tiden det tar å bryte seg gjennom de ulike fysiske barrierene er lengre enn summen av tiden det tar å detektere og varsle innbruddet, og den tiden det tar før reaksjonsstyrken (vekter, politi etc.) kan være på lokasjonen.

Dersom balansert sikring ikke kan oppnås skal oppdragsgiver ta stilling til om det er nødvendig å forsterke de eksisterende fysiske sikringstiltakene (grunnsikringstiltak) eller etablere ytterligere tiltak (påbyggingstiltak) for å redusere restrisiko til et akseptabelt nivå.

5.1.2. Godkjenning av skjermingsverdig informasjonssystem

NSM er godkjenningsmyndighet for skjermingsverdige informasjonssystemer som er angitt i virksomhetsikkerhetsforskriften § 51 første og andre ledd. Skjermingsverdige informasjonssystemer som ikke er nevn i første og andre ledd skal godkjennes av leverandøren, men oppdragsgiver skal gi tillatelse før informasjonssystemet kan tas i bruk.

Leverandøren skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. I virksomhetsikkerhetsforskriften § 49 stilles det funksjonelle krav for skjermingsverdig informasjonssystemer. Ved å følge NSMs og Forsvarsbyggs veiledere for godkjenning av informasjonssystemer anses kravene § 49 som ivaretatt.

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

Tempestrisikovurdering må utarbeides i tillegg til dokumentasjonen som er aktuell for skjermingsverdig informasjonssystem på BEGRENSET nivå. Oppdragsgiver kan fremskaffe mal for Tempestrisikovurdering.

5.1.3 Leverandørklarering

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.

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

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

5.1.4 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 som sikkerhetsklarering gjelder også for leverandørpersonell som har behov for tilgang til skjermingsverdig objekt eller skjermingsverdig infrastruktur.

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

Leverandøren må påregne minimum tre måneders saksbehandlingstid for sikkerhetsklarering av personell som kun er norske statsborgere. Saksbehandlingstiden regnes fra korrekt utfylt personopplysningsblankett (POB) er mottatt av klareringsmyndigheten.

En person som har utenlandsk statsborgerskap, kan etter en konkret helhetsvurdering få sikkerhetsklarering, 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.

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

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

Det gjøres oppmerksom på at det er leverandørens risiko at autorisasjon eller sikkerhetsklarering ikke oppnås. Han har også risikoen for at autorisasjon eller sikkerhetsklarering tar lengre tid enn 3 måneder, med mindre forsinkelsen skyldes forhold oppdragsgiver eller norske sikkerhetsmyndigheter svarer for.

5.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå eller høyere

Ved inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå eller høyere forplikter leverandøren seg til å oppfylle de krav som gjelder for angitt sikkerhetsgradering i tillegg til de krav som stilles ved inngåelse av sikkerhetsavtaler på BEGRENSET nivå.

5.2.1. 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.

5.2.2. Ytterligere krav

Det understrekes at ovennevnte krav ikke er uttømmende. I enkelte anskaffelser kan det, med bakgrunn i økt risiko knyttet til verdier, trusler eller sårbarheter bli stilt ytterligere krav til sikkerhet, jf. generelle krav til beskyttelse av skjermingsverdige verdier i virksomhetsikkerhetsforskriften kapittel 3.

5.2.3. NSMs veiledere og håndbøker

For leverandører med sikkerhetsavtale på KONFIDENSIELT nivå eller høyere vil samtlige av NSMs veiledninger og håndbøker være relevante å benytte i det forebyggende sikkerhetsarbeidet, se https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/.