



KONKURRANSEGRUNNLAGETS DEL III

OPPDRAGET NS 8403

Prosjektnavn: Byggeledelse – Portefølje 1001
Prosjektnummer: 100651
Kontraksnummer: C01810

Vedlegg:

- Orientering til leverandører om krav til håndtering og beskyttelse av skjermingsverdig informasjon i forbindelse med anskaffelser
- Ytelsesbeskrivelse

INNHold

1 INNLEDNING	3
2 ORIENTERING OM OPPDRAGET (KONTRAKTEN)	3
2.1 Beskrivelse av aktuelle bygg- og anlegg	3
2.2 Planlagt entreprisform	3
2.3 Oppdragets omfang	3
2.4 SHA koordinering i utførelsesfasen	3
2.5 Opsjoner	4
2.6 Anslått tidsforbruk	4
2.7 Avklaringer mot bruker	4
3 ORGANISATORISKE FORHOLD	4
3.1 Byggeleders organisasjon	4
3.2 Grensesnitt mot andre aktører	4
3.3 Byggeplass og møtested	4
4 ØKONOMISKE FORHOLD	5
4.1 Honorarform	5
4.2 Prisregulering	5
4.3 Reisekostnader	5
5 FREMDRIFT	5
6 KVALITETSSIKRING AV BYGGELEDERS LEVERANSE	5
6.1 Kvalitetsplan	5
6.2 Kontrollplan	5
7 FAKTURERING	6
7.1 Innledning	6
7.2 Krav til fakturaene	6
8 SPRÅK	6
9 SIKKERHET	7
9.1 Krav til beskyttelse av skjermingsverdig informasjon, skjermingsverdige informasjonssystemer og skjermingsverdige objekter og infrastruktur	7
9.2 Krav til autorisasjon, og eventuell adgangsklarering/sikkerhetsklarering av personell	7
10 INFORMASJON - PROFILERING	7
VEDLEGG 1 - ORIENTERING TIL LEVERANDØRER OM KRAV TIL HÅNDTERING OG BESKYTTELSE AV SKJERMINGSVERDIG INFORMASJON I FORBINDELSE MED ANSKAFFELSER	8

1 INNLEDNING

Forsvarsbygg er et forvaltningsorgan underlagt Forsvarsdepartementet. Forsvarsbygg er en av Norges største eiendomsaktører, og totalleverandør av eiendomstjenester til Forsvaret. Nærmere informasjon om Forsvarsbygg finnes på www.forsvarsbygg.no.

2 ORIENTERING OM OPPDRAGET (KONTRAKTEN)

2.1 Beskrivelse av aktuelle bygg- og anlegg

Oppdragsgiver skal inngå kontrakt om 1 byggeleder til 1 prosjekt i portefølje 1001.

Prosjektet omfatter nytt betongbygg over en etasje med bruttoareal på ca. 75 kvm. Det tekniske bygget har et behov for omfattende elektrotekniske arbeider, samt VVS tekniske isvanssledninger. Terrenget består av fjell, og sprengning må påregnes. Bygget vil også ha behov for sikringstiltak samt EMP tekniske tiltak. Prosjektet gjennomføres etter NS 8405. Forventet oppstart er i slutten av februar 2020.

Forsvarsbygg forutsetter at byggeleder har betydelig kompetanse og erfaring med tilsvarende prosjekter, herunder relevant erfaring fra bygg med omfattende tekniske arbeider, eksempelvis erfaring med sykehus. Tidligere erfaring med sikkerhetsgraderte prosjekter er en fordel.

Byggeleder bør ha kjennskap til:

- EMP- og tempestmessige tiltak
- Adgangskontroll/sikring av rom
- Branntekniske forhold og tiltak
- Ventilasjonsanlegg med gjennomføringer i spesielle vegger
- Kjøleanlegg for datainstallasjoner, kjøleutstyr, overskuddsvarme
- Elektrotekniske anlegg, tavler, vern, jording
- Nødstrømsaggregater
- Automasjon og SD anlegg
- Brannsløkkeanlegg med gass
- Evt. også fortifikasjonsmessige tiltak i bygg/ anlegg

2.2 Planlagt entrepriseform

Prosjektene vil i hovedsak utføres som Generalentrepriser.

2.3 Oppdragets omfang

Byggelederoppdraget omfatter ytelser i følgende faser i samsvar med prosjektets fremdrift:

- Utførelsesfasen
- Overtakelsesfasen
- Innredningsfasen

Ytelsesbeskrivelse:

- Oppdraget er nærmere spesifisert i vedlagte ytelsesbeskrivelse.

2.4 SHA koordinering i utførelsesfasen

- Byggeleder kan bli tildelt rollen som SHA-koordinator i utførelsesfasen. Det inngås i så fall egen avtale om dette.

2.5 Opsjoner

Kontrakt med byggeleder vil i tillegg til beskrevet prosjekt omfatte opsjon på ytterligere 2 prosjekter i porteføljen. Prosjektene vil ha flere av egenskapene til innledende prosjekt.

Prosjekt 2 – Forventet byggestart: Mars 2020

Prosjekt 3 – Forventet byggestart: August 2020

Forventet avslutning på opsjonene er desember 2021.

Forsvarsbygg står fritt til å avgjøre om opsjonsytelsene skal utføres eller ikke, eller eventuelt settes bort til andre leverandører.

2.6 Anslått tidsforbruk

Anslått omfang av byggeleders ytelser i de enkelte faser er:

Utførelsesfasen:	Antatt behov for fysisk tilstedeværelse 10-15 timer pr. uke.
Overtakelsesfasen:	Antatt behov for fysisk tilstedeværelse 10-15 timer pr. uke.
Innredningsfasen:	Antatt behov for fysisk tilstedeværelse 10-15 timer pr. uke.

Tidsforbruk er kun et anslag, og er ikke en bindende forutsetning for kontrakten mellom partene.

2.7 Avklaringer mot bruker

Ved oppstart av prosjektet vil det bli holdt et oppstartsmøte der alle relevante data fra brukere, parallelle prosjekter etc. gjennomgås. Det må påberegnes en kontinuerlig dialog med bruker og prosjektledelsen hos Forsvarsbygg. Disse vil bidra til avklaringer i forhold til behov, funksjon, standard og lignende.

3 ORGANISATORISKE FORHOLD

3.1 Byggeleders organisasjon

Det skal tilbys byggeledelse som dekker nødvendige fag slik at samtlige krav i kontrakten nås. Det skal tilbys 1 navngitt byggeleder.

Ved gjennomføringen av oppdraget er byggeleder forpliktet til å benytte tilbudte navngitt person til utførelsen av oppdraget.

3.2 Grensesnitt mot andre aktører

I byggefase vil det bli kontakt mot flere aktører, bl.a.

- Bruker
- Prosjekterende
- Entreprenør
- Leverandører av innredning og IKT

3.3 Byggeplass og møtested

Adresser for byggeplass og møtested er:

Byggeplass:	Oslo-regionen
-------------	---------------

Møtested:	Prosjektkontor
-----------	----------------

Forsvarsbygg stiller nødvendige kontorfasiliteter til disposisjon for gjennomføring av oppdraget. Byggeleder må disponere egen PC for dokumenthåndtering og kommunikasjon (epost).

4 ØKONOMISKE FORHOLD

4.1 Honorarform

Oppdraget honoreres etter medgått tid.

Byggeleder skal i samarbeid med oppdragsgiver utarbeide honorarbudsjetten for oppdraget, se konkurransegrunnlaget del II.

4.2 Prisregulering

Prisene reguleres i samsvar med bestemmelsen i konkurransegrunnlaget del II

4.3 Reisekostnader

Tilbudte priser skal dekke kostnader i forbindelse med reiser, og evt. overnatting, til og fra byggeplass, samt evt. møter på andre lokasjoner i Oslo-regionen.

Reisekostnader utover dette dekkes bare dersom Forsvarsbygg på forhånd har godkjent reisen.

5 FREMDRIFT

Forsvarsbygg har satt følgende tentative tidsplan* for gjennomføringen av oppdraget:

Nr.	Fase:	Dato fra	Dato til
1	Kontraktsinngåelse	Ultimo februar 2020	
3	Utførelsesfasen	Ultimo februar 2020	
4	Overtakelsesfasen	Juni 2020	
5	Evt. opsjoner	Etter avtale	

*Kontraktens varighet følger prosjektets faktiske fremdrift.

6 KVALITETSSIKRING AV BYGGELEDERS LEVERANSE

6.1 Kvalitetsplan

Byggeleder skal i prosjektet ha implementert en kvalitetsplan for å sikre at egne arbeider utføres i henhold til gjeldende forskrifter og kontraktens krav. Kvalitetsplanen skal oversendes oppdragsgiver senest 4 uker etter kontraktsinngåelse. Kvalitetsplanen skal holdes oppdatert i hele kontraktsperioden.

6.2 Kontrollplan

Byggeleder skal utarbeide kontrollplan for rutinemessige og spesielle kvalitetskontroller som skal utføres for å verifisere at kontraktens krav, gjeldene offentligrettslige krav samt kvalitetsplan oppfylles. Kontrollplanen skal også omfatte de kvalitetskontroller som byggeleder skal utføre for å verifisere at Forsvarsbyggs kontrakt med entreprenørene, og entreprenørenes etterlevelse av offentligrettslige krav, oppfylles.

Kontrollplanen skal minimum angi:

- Område (fag / funksjon / del / ...)
- Aktivitet/sjekkpunkt (arbeidsoperasjon / leveranse / ytelse / ...)
- Kontrollgrunnlag (krav / referanse /...)
- Hvordan (prosedyre / sjekklister / ...)
- Tidspunkt (fast rutine / tidsfrist / milepæl / ...)
- Ansvarlig (utførende / godkjenning / ...)
- Varsling (byggherre / myndighet / ...)
- Dokumentasjon (dokumentasjonskrav)

Kontrollplanen skal oversendes Forsvarsbygg senest fire uker etter kontraktsinngåelse.

Forsvarsbygg vil angi på byggeleders kontrollplaner hvilke aktiviteter/sjekkpunkter Forsvarsbygg skal delta på og rapportere dette tilbake til byggeleder.

Byggeleder skal dokumentere at kontroll i henhold til planen er foretatt, og at resultatet er i samsvar med gitte krav. Avvik som kontrollene avdekker skal registreres og rapporteres fortløpende til Forsvarsbygg. Oppdatert kontrollplan skal oversendes Forsvarsbygg månedlig.

Dokumentasjon av kvalitetskontroll i form av registreringer (utfylte kontrollplaner med sjekklister/kontrollskjemaer) arkiveres hos byggeleder i hele bygge- og reklamasjonstiden, og tas inn i FDV-dokumentasjonen.

7 FAKTURERING

7.1 Innledning

Faktura og kreditnota skal sendes elektronisk til Forsvarsbyggs fakturamottak i samsvar med standarden Elektronisk handelsformat (EHF). Forsvarsbyggs elektroniske fakturaadresse er **975950662**. For nærmere informasjon om fremgangsmåte, se www.ehandel.no.

Spesifiserte oppgaver i henhold til NS 8403 punkt 10.2.4 skal vedlegges alle fakturaer. Det skal sendes separate fakturaer for:

- Endringsarbeid
- Slutfaktura

Forsvarsbyggs betalingsbetingelser er 28 dager etter mottak av faktura.

7.2 Krav til fakturaene

Alle fakturaer skal inneholde:

- «xxx» - oppgis under «Deres referanse» («AccountingCustomerParty»/«Party»/«Contract ID»)
- «Prosjektnummer 100255, kontraktsnr.» – oppgis i beskrivelsesfeltet
- Faktura for endringsarbeider skal i beskrivelsesfeltet i tillegg henviser til endringsavtalenummer (E001, E002 osv.).
- Videre skal beskrivelsesfeltet inneholde opplysninger om hvilke ytelser/leveranser fakturaen gjelder. Fakturaene skal spesifiseres og dokumenteres slik at de kan kontrolleres av oppdragsgiveren.

Ved manglende eller feil merking vil byggeleder kunne få beskjed om at den umerkede/feilmerkede fakturaen ikke vil bli behandlet. Byggeleder plikter da å kreditere den umerkede fakturaen og utstede en ny korrekt faktura med ny fakturadato og nytt forfall.

8 SPRÅK

Alle dokumenter, møtereferater mv. skal fremlegges på norsk. Muntlige fremstillinger og presentasjoner vil også foregå på norsk.

9 SIKKERHET

Gjennomføringen av kontrakten er underlagt sikkerhetsrestriksjoner i henhold til sikkerhetslovens bestemmelser, se punkt 9.1 til 9.2.

Det stilles krav om at byggelederen må være et norsk foretak eller foretak fra stat som Norge har et sikkerhetspolitisk samarbeid med.

9.1 Krav til beskyttelse av skjermingsverdig informasjon, skjermingsverdige informasjonssystemer og skjermingsverdige objekter og infrastruktur

Krav til beskyttelse av skjermingsverdig informasjon (ugradert eller sikkerhetsgradert), skjermingsverdige informasjonssystemer og skjermingsverdige objekter og infrastruktur er gitt i vedlegg 1.

For beskyttelse av skjermingsverdig informasjon sikkerhetsgradert KONFIDENSIELT eller høyere, se hele vedlegg 1.

9.2 Krav til autorisasjon, og eventuell adgangsklarering/sikkerhetsklarering av personell

Under gjennomføringen av kontrakten vil byggelederen få tilgang til eller tilvirke skjermingsverdig informasjon, eller få tilgang til et skjermingsverdig objekt eller infrastruktur i henhold til sikkerhetsloven.

For denne kontrakten gjelder følgende:

Leverandørpersonell har behov for tilgang til skjermingsverdig objekt eller infrastruktur, og skal inneha nødvendig autorisasjon og adgangsklarering/sikkerhetsklarering.

Krav til autorisasjon og sikkerhetsklarering for informasjon sikkerhetsgradert HEMMELIG.

Nærmere informasjon om autorisasjon og eventuell adgangsklarering/sikkerhetsklarering knyttet til gjennomføring av kontrakten vil bli gitt ved henvendelse til byggherren.

10 INFORMASJON - PROFILERING

All kontakt med media og publikum skal håndteres av oppdragsgiver. Henvendelser fra media, eller forespørsler om innsyn, skal henvises til oppdragsgivers prosjektleder eller annen oppgitt kontaktperson for slike henvendelser.

Dersom byggeleder eller noen av byggelederens kontraktsmedhjelpere for reklameformål eller annen måte ønsker å gi offentligheten informasjon om oppdraget, skal dette alltid forelegges oppdragsgiver på forhånd til godkjenning.

Vedlegg 1 - 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
4.1.1.	Autorisasjon	4
4.1.2.	Autorisasjon av utenlandsk statsborger	5
4.1.3.	Beskyttelse av skjermingsverdige informasjonssystemer.....	5
4.1.4.	Dokumentasjon av at kravet til forsvarlig sikkerhetsnivå er oppnådd	5
4.2.	Inngåelse av sikkerhetsavtale på BEGRENSET nivå.....	5
4.2.1.	Unntak fra krav om sikkerhetsavtale	5
4.2.2.	Innholdet i sikkerhetsavtalen.....	5
4.2.3.	Brudd på sikkerhetskrav	6
4.2.4.	Ytterligere sikkerhetskrav	6
4.2.5.	Veiledere.....	6
5.	Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå eller høyere	6
5.1.	Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT eller høyere	6
5.1.1.	Soneinndeling for informasjon gradert KONFIDENSIELT eller høyere	7
5.1.2.	Leverandørklarering.....	7
5.1.3.	Sikkerhetsklarering og autorisasjon av leverandørpersonell.....	7
5.2.	Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå eller høyere	8
5.2.1.	Godkjenning av informasjonssystem	8
5.2.2.	Brudd på sikkerhetskrav	8
5.2.3.	Ytterligere krav	8
5.2.4.	Veiledere.....	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 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 infrastruktur.

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

Sikkerhetsstruende 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 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 og 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 objekt eller infrastruktur. I den forbindelse vil oppdragsgiver gi råd og veiledning om forebyggende sikkerhetstjeneste.

1.4. Hjemmel

Lov om nasjonal sikkerhet (sikkerhetsloven) gjelder for statlige, fylkeskommunale og kommunale organer, samt leverandører av varer og tjenester ifm|sikkerhetsgraderte anskaffelser.

Sentrale forskrifter som er hjemlet i sikkerhetsloven:

- Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften)
- Forskrift om sikkerhetsklarering og annen klarering (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

En virksomhet som omfattes av sikkerhetsloven, skal etablere et styringssystem for sikkerhet. Systemet skal sikre at virksomheten som oppfyller kravene gitt i eller med hjemme i loven.

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 forskrift om sikkerhetsklarering og annen klarering av 20. desember 2018 (klareringsforskriften) § 31).

1.5.5. Brudd på sikkerhetskrav

Overtredelse av sikkerhetsbestemmelser, forsettlig eller uaktsomt, kan ansees 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 følgende veiledere utgitt av NSM være relevante å benytte i det forebyggende sikkerhetsarbeidet.

- Veileder i sikkerhetsstyring
- Veiledning i risikovurderinger
- Veiledning i sikkerhetsrevisjoner

Veiledninger fra NSM til den nye sikkerhetsloven blir publisert fortløpende i 2019 på NSM sine sider, se <https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/>. Så langt de passer kan veiledninger utarbeidet til tidligere sikkerhetslov benyttes inntil nye foreligger.

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 behandle eller oppbevare 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.

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

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 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.

4.1.2. 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, 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.

4.1.3. Beskyttelse av skjermingsverdige informasjonssystemer

Leverandøren skal sørge for et forsvarlig sikkerhetsnivå for skjermingsverdige informasjonssystemer. I virksomhetsikkerhetsforskriften § 49 stilles det funksjonelle krav for skjermingsverdige informasjonssystemer.

4.1.4. Dokumentasjon av at kravet til forsvarlig sikkerhetsnivå er oppnådd

Før sikkerhetsavtale kan inngås skal leverandøren dokumentere at han på en tilfredsstillende måte både har vurdert og håndtert risiko og hvilke sikkerhetstiltak som er etablert for

- lokaler som skal brukes til oppbevaring og behandling av dokumenter og lagringsmedier inneholdende informasjon gradert BEGRENSET
- informasjonssystemer som skal brukes til behandling av informasjon gradert BEGRENSET

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 skjermingsverdige objekt eller infrastruktur i eller fra sine egne lokaler.

4.2.1. 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.

4.2.2. 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 påse 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 sikkerhetsinstruksjoner 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 skjeringsverdig 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 oppfylder kontraktsforpliktelser knyttet til forebyggende sikkerhetstjeneste
- legge til rette for at NSM eller sektormyndighet med tilsynsansvar kan kontrollere sikkerhetstilstanden hos leverandøren

4.2.3. 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.

4.2.4. 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 skjeringsverdige verdier i virksomhetsikkerhetsforskriften kapittel 3.

4.2.5. Veiledere

For leverandører med sikkerhetsavtale på BEGRENSET nivå vil følgende NSM veiledninger, i tillegg til de som er nevnt ovenfor, være relevante å benytte i det forebyggende sikkerhetsarbeidet.

- Veiledning i sikkerhetsgraderte anskaffelser
- Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon
- Veiledning i sikkerhetsgodkjenning
- Veileder i fysisk sikring
- Håndtering av uønskede hendelser
- Veiledning til sikkerhetsloven kapittel 8 og bestemmelser om personellsikkerhet i forskriftene

Det anbefales at «Veileder i håndtering og beskyttelse av sikkerhetsgradert informasjon», «Veiledning i sikkerhetsgodkjenning» og «Veileder i fysisk sikring» ses i sammenheng.

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 for håndtering og beskyttelse av informasjon gradert KONFIDENSIELT eller høyere kommer i tillegg til kravene som gjelder for håndtering og beskyttelse av 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.

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.

Dersom leverandøren skal ha et område med direkte tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal det etableres en sperret sone rundt området.

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 sikkerhetsklart 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. Leverandørklarering

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

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

5.1.3. Sikkerhetsklarering og autorisasjon av leverandørpersonell

Før leverandørklarering kan gis skal leverandørens leder og styremedlemmer sikkerhetsklareres for det samme nivå som det er anmodet om leverandørklarering for. En leverandørklarering kan likevel gis dersom det styremedlem eller leverandørens leder som ikke kan sikkerhetsklareres, gir avkall på retten til innsyn i den sikkerhetsgraderte informasjonen eller tilgangen til objekter eller infrastruktur som gjør det nødvendig med leverandørklarering.

Leverandøren må påregne minimum tre måneders saksbehandlingstid for sikkerhetsklarering av personell som kun er norske statsborgere. Tre måneders fristen 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 i § 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.

Leverandørens leder skal sørge for at eget personell som har tjenstlig behov for tilgang til sikkerhetsgradert informasjon som leverandøren er i besittelse av, blir autorisert. Ved behov for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må det kontrolleres at vedkommende har gyldig sikkerhetsklarering for den aktuelle sikkerhetsgraden.

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 sikkerhetsavtaler på BEGRENSET nivå.

5.2.1. Godkjenning av informasjonssystem

Informasjonssystem som skal behandle sikkerhetsgradert informasjon på KONFIDENSIELT nivå skal godkjennes av oppdragsgiver før de tas i bruk. NSM godkjenner informasjonssystem med høyere graderingsnivå.

5.2.2. 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.

5.2.3. 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.

5.2.4. Veiledere

For leverandører med sikkerhetsavtale på KONFIDENSIELT nivå vil samtlige veiledninger som er nevnt ovenfor være relevante å benytte i det forebyggende sikkerhetsarbeidet.