FORSVARSBYGG

KONKURRANSEGRUNNLAGETS DEL III

OPPDRAGET
NS 8403

Vågsøy

Prosjektnavn: P2078 – Byggeledelse
Prosjektnummer: 100802
Kontraktsnummer: C04525

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 entrepriseform 3
2.3 Oppdragets omfang 4
2.4 SHA koordinering i utførelsesfasen 4
2.5 Anslått tidsforbruk 4
2.6 Avklaringer mot bruker 4

3 ORGANISATORISKE FORHOLD 4

3.1 Forsvarsbyggs organisasjon 4
3.2 Byggeleders organisasjon 5
3.3 Grensesnitt mot andre aktører 5
3.4 Byggeplass og møtested 5

4 SAMHANDLING OG FLYT I PROSJEKTET 5

4.1 Sentrale elementer i *Flyt i prosjektene* 5
4.1.1 Omforente fremdriftsplaner ved hjelp av involverende planlegging og Lean Construction 6
4.1.2 Møter i prosjektet 6
4.1.3 Systematisk ferdigstillelse 6
4.2 Samhandling med kontraktspart 6
4.3 Prosess frem mot oppstart utførelse 6
4.4 Flyt på byggeplassen - tavlemøter 7

5 ØKONOMISKE FORHOLD 8

5.1 Honorarform 8
5.2 Prisregulering 8
5.3 Reisekostnader 8

6 FREMDRIFT 8

7 KVALITETSSIKRING AV BYGGELEDERS LEVERANSE 9

7.1 Kvalitetsplan 9
7.2 Kontrollplan 9

8 SPRÅK 9

9 SIKKERHET 9

9.1 Byggelederens behov for til tilganger til skjermingsverdige verdier 9
9.2 Tilgang til skjermingsverdig informasjon i byggelederens egne lokaler 10
9.3 Tilgang til skjermingsverdige verdier hos oppdragsgiveren 10
9.4 Avtale om håndtering og beskyttelse av ugradert skjermingsverdig informasjon og skjermingsverdig ugradert informasjonssystem 10
9.5 Krav til sikkerhetsavtale mellom oppdragsgiveren og byggeleder, og eventuell leverandørklarering 10
9.6 Krav til autorisasjon, og eventuell sikkerhetsklarering av personell 11

10 INFORMASJON - PROFILERING 11

VEDLEGG 1 - ORIENTERING TIL LEVERANDØRER OM KRAV TIL HÅNDTERING OG BESKYTTELSE AV SKJERMINGSVERDIG INFORMASJON I FORBINDELSE MED ANSKAFFELSER 12

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.

Forsvarsbygg har høyt fokus på god flyt i prosjektene. Formålet er at prosjektene skal bidra til økt forsvarsevne gjennom bedre leveranser, høyere kvalitet og mer effektiv gjennomføring. Vi benytter filosofi, metodikk og verktøy fra Lean Construction, og Systematisk ferdigstillelse for å oppnå dette. Vi kaller dette «Flyt i prosjektene» i Forsvarsbygg. Det er forventet at alle kontraktsparter i våre EBA-prosjekter benytter denne metodikken. Dette er nærmere beskrevet i kapittel 4 og i ytelsesbeskrivelsen.

I juni 2019 vedtok Stortinget å investere i nye radarer for å overvåke norsk og nærliggende luftrom. Prosjektet krever et tett samarbeid mellom flere aktører i forsvarssektoren; Forsvarsmateriell, Forsvarsbygg, Forsvarsstaben (FST), Luftforsvaret og Forsvarsdepartementet.

Forsvarsbygg skal etablere 8 nye radarstasjoner i prosjektet. Den første stasjonen som skal bygges er i Vågsøy i Kinn kommune. Til bygging av ny radarstasjon på Vågsøy ønsker Forsvarsbygg tilbud på byggeledelse.

2 ORIENTERING OM OPPDRAGET (KONTRAKTEN)

2.1 Beskrivelse av aktuelle bygg- og anlegg

Radarstasjonen skal bygges etter krav og spesifikasjoner gitt av Luftforsvaret og Forsvarsmateriell.

Det skal i perioden 2024-2025 bygges nytt bygg på Vågsøy.

Arbeidene som skal gjennomføres er etablering av et bygg med en indre betongkjerne og et ytre skall av stål og tre/aluminiums-kledning. Det ytre skallet skal blant annet inneholde garasjering.

Det skal en rekke tekniske anlegg inn i bygget som planlegges gjennomført som en generalentreprise (bygg, elektro, rør og ventilasjon).

Bygget ligger på en fjelltopp ved eksisterende radarstasjon og det er etablert grusvei opp til tomten.

Ved behov kan det være aktuelt å benytte byggeleder også inn mot andre lokasjoner i programmet 2078.

2.2 Planlagt entrepriseform

Byggeprosjektet planlegges utført med en generalentreprise for bygg, elektro, rør og ventilasjon, med diverse byggherrestyrte delte entrepriser. Byggeleder vil etter behov bistå med koordinering av byggherrestyrte delte entrepriser. Adkomtsveg med infrastruktur og tomteopparbeidelse inngår i egen entreprise som ble igangsatt i 2022. Videre entrepriser vil være:

- Reservekraft
- Kjølemaskiner
- SD/SRO
- Elektronisk sikring
- Brannalarm
- Lås og beslag
- Trafo
- Brannslokking
- Dører og gitter
- Leveranser FMA/Cyfor

2.3 Oppdragets omfang

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

☒ Detaljprosjekterings- og anskaffelsesfasen – disse fasene pågår, men byggeleder vil bli involvert i avslutningen av disse fasene

☒ Utførelsesfasen

☒ Overtakelsesfasen

☒ Prøvedriftsfasen (etter behov)

☒ Reklamasjons- og garantifasen (etter behov)

Ytelsesbeskrivelse:

Oppdraget vil bli spesifisert etter kontraktsinngåelsen, med utgangspunkt i vedlagte ytelsesbeskrivelse.

2.4 SHA koordinering i utførelsesfasen

Byggeleder skal ivareta rollen som SHA-koordinator i utførelsesfasen.

2.5 Anslått tidsforbruk

Anslått omfang av byggeleders ytelser i de enkelte faser er:

Detaljprosjekterings- og anskaffelsesfasen:	Ca 50 %
Utførelsesfasen:	70 – 100 %
Overtakelsesfasen:	Ca 100 %
Prøvedriftfasen:	Etter behov
Reklamasjons- og garantifasen:	Etter behov

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

2.6 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 Forsvarsbyggs organisasjon

Forsvarsbyggs organisasjon er organisert slik:

Funksjon	Firma	Kontaktperson
Prosjektsjef prosjekt P2078	Forsvarsbygg	Anders Martinsen
Totalprosjektleder prosjekt P2078	Forsvarsbygg	Ylva Sneve
Prosjektleder Vågsøy bygg	Forsvarsbygg	Frode Oppheim / Daniel Morken
Prosjekteringsgruppekoordinator	Sweco AS	Per Christian Bruu
Prosjektkoordinator bruker	Luftforsvarsstaben	Jostein Kleiven

Prosjektkoordinator	Forsvarsbygg Eiendomsforvaltning	Alf Gustav Høstmark

3.2 Byggeleders organisasjon

Det skal tilbys byggeledelse med tverrfaglig kompetanse som dekker nødvendige fag slik at samtlige krav i kontrakten nås, iht. pkt. 2 overfor.

Det skal tilbys en navngitt byggeleder.

Ved gjennomføringen av oppdraget er leverandøren forpliktet til å benytte den tilbudte navngitte personen til utførelsen av oppdraget.

3.3 Grensesnitt mot andre aktører

Prosjektet har en rekke grensesnitt mot andre aktører og interne grensesnitt mellom ulike kontrakter. Vesentlige grensesnittaktører er Forsvarsmateriell med sine eksterne leverandører og Forsvarets IT-avdeling (FMA IKT og Cyfor).

Det er ikke tatt standpunkt til tiltransport av tekniske entrepriser. Byggelederytelsen kan komme til å omfatte koordinering mellom alle entrepriser.

3.4 Byggeplass og møtested

Adresser for byggeplass og møtested er:

Byggeplass:	Vågsøy i Kinn kommune
Møtested:	Vågsøy - Byggeplass på fjelltoppen Heida/Kvalheimsfjellet

Forsvarsbygg stiller kontor til disposisjon i entreprenørrigg på byggeplass i den tiden av oppdragsperioden hvor denne er oppe. Kontorarbeid i egne lokaler og på Forsvarsbyggs kontor i Oslo eller Bergen kan påregnes.

4 Samhandling og Flyt i prosjektet

.

4.1 Sentrale elementer i *Flyt i prosjektene*

Byggeledelsen har en sentral rolle i implementeringen og gjennomføring av Flyt i prosjektet, i tråd med prinsippene som er skissert i dette kapittelet. Forsvarsbygg har også tydelige krav i til prosjekterende og entreprenør, og nedenfor følger en kortfattet versjon av dette med spesielt fokus på byggeledelsen sin rolle. Forsvarsbygg har utarbeidet en egen Veileder for Flyt i prosjektene med tilhørende maler. Denne vil byggeledelsen få tilgang til ved oppstart.

Med begrepet «Flyt i prosjektet» menes anvendelse av Forsvarsbyggs filosofi, metoder og verktøy for å oppnå bedre leveranser, høyere kvalitet og mer effektiv gjennomføring av prosjektene. Disse er basert på Lean Construction og Systematisk ferdigstillelse. I tillegg er det fokus på samhandling og kontinuerlig forbedring gjennom oppdraget.

De viktigste elementene i dette er

- Omforente fremdriftsplaner ved hjelp av involverende planlegging og Lean Construction (jf. pkt. 4.1.1)Møter i prosjektet (jf. pkt. 4.1.2)
- Systematisk ferdigstillelse (jf. pkt. 4.1.3)
- Samhandling med kontraktspart (jf. pkt. 4.2)

- Prosess frem mot oppstart utførelse (jf. pkt. 4.3)
- Flyt på byggeplassen (jf. pkt. 4.4)

4.1.1 Omforente fremdriftsplaner ved hjelp av involverende planlegging og Lean Construction

Prosjekterende og entreprenør skal utarbeide omforente, detaljerte fremdriftsplaner, både for prosjektering (ved NS 8407) og bygging. Planen utarbeidet basert på Lean-metodikk (som f.eks. taktplanlegging, involverende planlegging og bakoverplanlegging). Ved bruk av involverende planlegging involvere alle deltakerne i prosjektet, slik at de har større grad av eierskap til fremdriftsplaner for prosjektering og byggefase. Deltakerne skal bli enige om leveranser, rekkefølge på aktiviteter i gjennomføringen, ansvarsfordeling og avhengigheter mellom ulike aktiviteter.

Deltakerne som skal involveres inkluderer blant annet anleggsledere/formenn/baser, eventuelle underentreprenører, nøkkelressurser i prosjekteringsgruppen, driftsorganisasjonen, og byggherrens prosjektorganisasjon. Byggeledelsen skal bidra til prosessene der involverende planlegging benyttes samt legge til rette for tilstrekkelig grad av involvering underveis i prosjektet.

4.1.2 Møter i prosjektet

For å oppnå effektive møter skal møter gjennomføres i henhold til en agenda som sendes ut før møtet, og som beskriver hva deltakerne skal forberede og hva som skal besluttes. Det gjennomføres jevnlig evaluering av møtene med formål om kontinuerlig forbedring av møtenes form og innhold. Evalueringene gjennomføres av møtearrangøren.

4.1.3 Systematisk ferdigstillelse

Forsvarsbygg har fokus på Systematisk ferdigstillelse, og byggeledelse så vel som prosjekterende og entreprenør skal sette seg godt inn i hva som forventes. Arbeidsoppgaver og krav følger av konkurransegrunnlagets Del III C-2 Plan for Systematisk ferdigstillelse (del av konkurransegrunnlag for entrepriser), «NS 3935:2019 – Integrerte Tekniske Bygningsinstallasjoner – Prosjektering, utførelse og idriftsettelse» og «NS6450:2016 – Idriftsetting og prøvedrift av tekniske bygginstallasjoner». Omfang og kompleksitet tilpasses prosjekt og faser i prosjektet.

4.2 Samhandling med kontraktspart

Det legges opp tett samhandling med entreprenørene og byggeledelsen har en sentral rolle i denne. Samhandling er en kontinuerlig prosess og bygger på åpenhet, tillit og det å arbeide mot felles mål. Disse verdiene skal prege partenes handlemåte under gjennomføring av oppdraget. God samhandling kjennetegnes av:

- Respekt for alle deltakerne i prosjektet
- Involvering av alle bidragsytere
- Stadig forbedring av prosesser – kontinuerlig forbedring og fokus på å være ett lærende prosjekt

Samhandlingen med entreprenør går gjennom hele kontraktgjennomføringen fra oppstart av kontrakten og frem til overlevert EBA. Samhandlingsfasen er den innledende klargjørende fasen etter signert kontrakt.

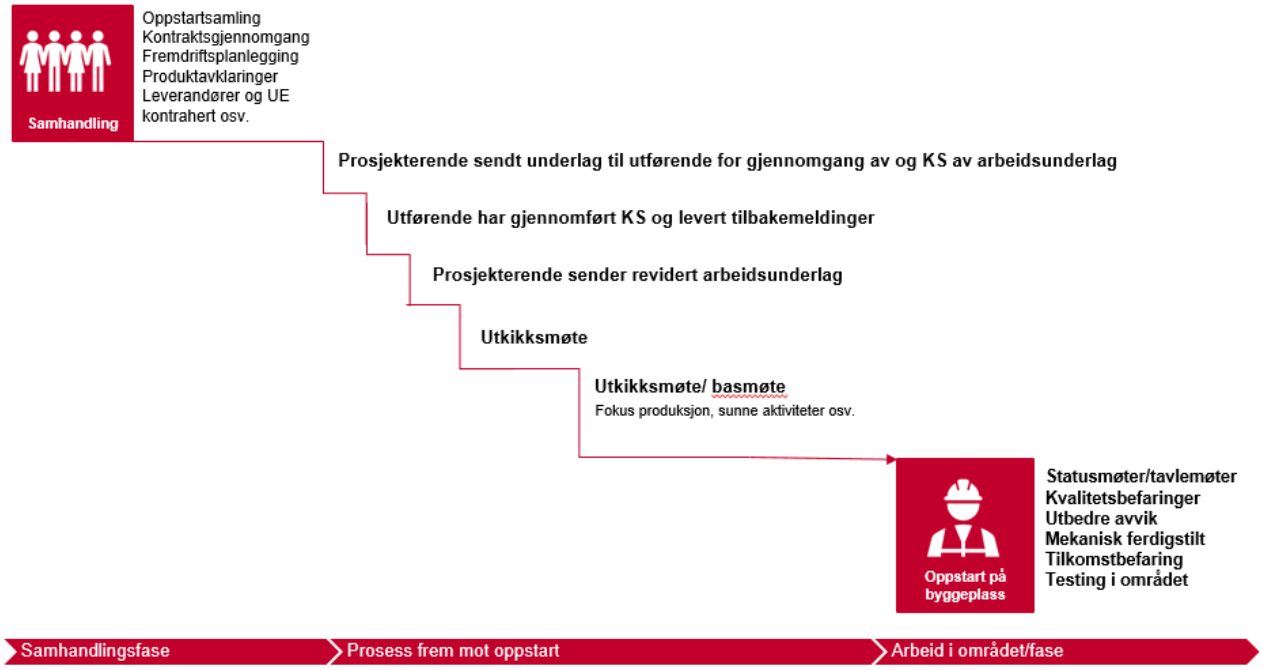
I tillegg til at byggeledelsen har en rolle i samhandling og samhandlingsfasen skal det også være en samhandling og oppstart med byggeledelsen når de kommer inn i prosjektet.

4.3 Prosess frem mot oppstart utførelse

I tillegg til avklaringer i samhandlingsfasen legges det opp til en prosess med møter, leveranser og nødvendige avklaringer frem mot oppstart av et gitt område eller fase. Inndeling i faser og områder defineres i forbindelse med

fremdriftsplanleggingen i samhandlingsfasen. Prosessen er illustrert i figuren nedenfor. Dersom Entreprenøren har egenutviklet systematikk kan denne benyttes etter avtale med Forsvarsbygg.

Hensikten er å avklare forhold knyttet til produksjon, gjennomføre nødvendig kvalitetssikring og sikre at alle er godt forberedt til oppstart i ett område eller en type arbeid. Entreprenør, rådgiver og byggherre har alle viktige oppgaver i denne prosessen, og byggeledelsen vil ha ansvar for å lede eller tett følge opp flere møter i prosessen.



Figur: Eksempel på prosess frem mot oppstart utførelse

Utkikksmøter

Før oppstart av byggearbeider i konkrete områder eller faser, skal entreprenøren ved NS8407 eller byggeleder ved NS8405kalle inn til såkalte utkikksmøter. I utkikksmøtet er formålet å kontrollere at forutsetningene for å utføre oppgavene er på plass, deriblant at det er planlagt med tilstrekkelig informasjon (tegninger, skjema etc.), materialer og bemanning.

Hver uke samles basene og byggeledelsen for å planlegge de kommende tre ukenes arbeid i detalj. Fokus her vil f.eks. være produksjon, arbeidspakker, sunne aktiviteter, tilkomstbefaring osv. Det henvises spesielt til sjekkliste for prosess frem mot oppstart i Veilederen for Flyt i prosjekter.

4.4 Flyt på byggeplassen - tavlemøter

Det gjennomføres korte statusmøter på byggeplass (tavlemøter) på ca. 15 minutters varighet. Ved NS8407 kaller entreprenøren inn til møtene, og byggeledelsen deltar etter behov. Dette kan også inngå i morgenmøter. Ved NS8405 har byggeleder ansvar for å kalle inn til tavlemøtene. Forsvarsbygg har egne veiledere og maler knyttet til dette. I perioder med stor aktivitet og flere aktører er det naturlig å ha dette daglig, i perioder med lavere aktivitet kan det være tilstrekkelig med 2-3 ganger i uken.

I disse møtene skal entreprenøren rapportere på status for fremdrift, SHA/HMS, kvalitet, bemanning, ryddighet/rent tørt bygg (RTB) og sikkerhet for ett gitt område etter trafikklysprinsippet:

- Grønt: Alt er iht. plan. Ingen nødvendige aksjoner.
- Gult: Usikkert eller uavklart, frist med tiltak (tiltak fremlegges).
- Rødt: Kritisk og vil ikke klare å ivareta som planlagt selv ved iverksetting av tiltak. Løftes til prosjektledelsen for å finne løsning.

Tilkomstbefaring

Ved oppstart av nye arbeider eller arbeid i nye områder skal det gjennomføres tilkomstbefaringer. Formålet med en tilkomstbefaring er blant annet å avdekke manglende ferdigstillelse, utilstrekkelig kvalitet eller uryddighet som kan hindre oppstart av nye arbeider i et område. Befaring gjennomføres med fagene som jobber i området og fagene som skal inn i området. Entreprenør kaller inn til befaringene, byggeleder deltar etter behov og spesielt i starten av kontraktsarbeidene.

5 ØKONOMISKE FORHOLD

5.1 Honorarform

Oppdraget honoreres etter medgått tid.

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

5.2 Prisregulering

Prisene reguleres i samsvar med bestemmelsen i konkurransegrunnlaget del II.

5.3 Reisekostnader

Tilbudte priser skal dekke reisetid og reisekostnader, herunder også kost og losji, i forbindelse med reiser til og fra byggplassen.

Reisetid og reisekostnader utover dette dekkes bare dersom Forsvarsbygg på forhånd har godkjent reisen.

6 FREMDRIFT

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

Nr.	Fase:	Dato fra	Dato til
1	Kontraktsinngåelse	Jan 2024	
2	Detaljprosjekterings- og anskaffelsesfasen	Løpende	Mars 2024
3	Utførelsesfasen	Mars 2024	Des 2025
4	Ferdigstillelse bygningsmessige arbeider	Okt 2025	
5	Overtakelse alle entrepriser	05.12.2025	
6	Prøvedriftsfasen	05.12.2025	05.12.2026
7	Reklamasjons- og garantifasen	5 år	

*Kontraktens varighet følger prosjektets faktiske fremdrift.

7 KVALITETSSIKRING AV BYGGELEDERS LEVERANSE

7.1 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.

7.2 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 inneholder aktiviter knyttet til kapittel 4. Samhandling og Flyt i prosjektet. Herunder er spesielt viktig å få med aktiviteter knyttet til prosess frem mot oppstart, tavlemøter og tilkomstbefaringer.

Kontrollplanen skal minimum angi:

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

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. I prosjekter der det benyttes digitale verktøy som muliggjøre digital kvalitetsoppfølging skal dette benyttes.

8 SPRÅK

Alle dokumenter, aksjonslister, 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.

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

9.1 Byggelederens behov for til tilganger til skjermingsverdige verdier

Oppdragsgiveren har tatt stilling til hva byggelederen kan få tilgang til av skjermingsverdig informasjon, informasjonssystemer, objekter eller infrastruktur (skjermingsverdige verdier).
Byggeleder har kun behov for tilgang til skjermingsverdige verdier hos oppdragsgiver.

Krav til beskyttelse av skjermingsverdig informasjon er gitt i vedlegg 1.

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

9.2 Tilgang til skjermingsverdig informasjon i byggelederens egne lokaler

Byggelederen vil ikke ha behov for å oppbevare eller behandle informasjon i papirform som er skjermingsverdig.
Byggelederen vil ikke ha behov for å behandle informasjon på informasjonssystem som er skjermingsverdig.
Informasjonssystem hos byggeleder som skal behandle skjermingsverdig informasjon skal godkjennes før det tas i bruk.
Informasjonssystem hos byggelederen vil ikke være tilknyttet skjermingsverdig objekt eller infrastruktur.

9.3 Tilgang til skjermingsverdige verdier hos oppdragsgiveren

Byggelederen vil ha behov for tilgang til skjermingsverdig informasjon (i papirform eller elektronisk) hos oppdragsgiveren uten oppsyn av representant for oppdragsgiveren. Informasjonen vil være sikkerhetsgradert KONFIDENSIELT.

Byggelederen vil ha behov for fysisk tilgang til skjermingsverdig objekt eller infrastruktur uten oppsyn av representant for oppdragsgiveren.

Byggherren planlegger med et eget rom for oppbevaring av tegninger. Alle tegninger som er utgått eller rødstrektegninger for as-bult etc leveres BH.

Et begrenset antall personer hos entreprenører på byggeplass vil få ansvar for tegningshåndtering. Byggeleder må også påregne ansvar for og kontroll av entreprenørers tegningshåndtering. Det vil utarbeides en egen dokumenthåndteringsplan og sikkerhetsinnstruks for byggeplass.

Byggeleders ansvar omfatter bl.a.:

- Kvittere mottatte tegninger.
- Kvittere tegninger som skal benyttes utenfor «tegningsbrakke» ut og inn hver dag og evt til lunsj. Det skal ikke ligge ubevoktede tegninger noe sted.
- Kvittere utgåtte tegninger.
- Kvittere rødstrektegninger som underlag for as-built

Tegninger gradert B kan medbringes til byggeplass og holdes i personlig varetekt.

9.4 Avtale om håndtering og beskyttelse av ugradert skjermingsverdig informasjon og skjermingsverdig ugradert informasjonssystem

Før byggelederen får tilgang til ugradert skjermingsverdig informasjon eller skjermingsverdig ugradert informasjonssystem, må byggelederen inngå en avtale med oppdragsgiveren. I avtalen fastsettes det hvordan byggelederen skal forholde seg til de kravene som gjelder for anskaffelsen.

For denne kontrakten gis det tilgang til både ugradert skjermingsverdig informasjon og skjermingsverdig ugradert informasjonssystem.

9.5 Krav til sikkerhetsavtale mellom oppdragsgiveren og byggeleder, og eventuell leverandørklarering

Før byggelederen gis tilgang til skjermingsverdige verdier er det krav til sikkerhetsavtale, men ikke krav til leverandørklarering.

9.6 Krav til autorisasjon, og eventuell sikkerhetsklarering av personell

Før byggelederens personell gis tilgang til skjermingsverdige verdier er det krav til autorisasjon og sikkerhetsklarering for informasjon sikkerhetsgradert HEMMELIG/NC.

Mobilbruk er ok i lompen, men ikke på byggeplass. Byggherre vil anskaffe et begrenset antall mobiler til bruk på byggeplass.

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

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 godkjennelse.

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
4.2. 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/.