



Konkurransesgrunnlagets del III-D - Administrative bestemmelser NS 8401

INNHOLDSFORTEGNELSE

1 KVALITETSSIKRING	2
1.1 Generelt	2
1.2 Kvalitetsplan	2
1.3 Kontrollplaner og sjekklister	2
1.4 Avviksbehandling	2
1.5 Revisjoner	3
2 FREMDRIFTSTIDSPPLANLEGGING, KOSTNADSSTYRING OG RAPPORTERING	3
2.1 Fremdriftsplan	3
2.2 Bemanningsplaner	3
2.3 Dokumentplan	3
2.4 Fremdriftsrapportering	3
2.5 Krav til planleggingsverktøy	3
2.6 Faktureringsplan	4
2.7 Kostnadsrapportering	4
2.8 Rapporteringsperiode/statusdato (kuttdato)	4
2.9 Rapportering	4
2.10 Endringsavtaler	4
3 FAKTURERING	4
3.1 Innledning	4
3.2 Krav til fakturaene	5
3.3 Krav til de ulike fakturakategoriene	5
4 SPRÅK	5
5 SIKKERHET	5
5.1 Prosjekterendes behov for tilgang til skjermingsverdige verdier	5
5.2 Tilgang til skjermingsverdig informasjon i prosjekterendeens egne lokaler	6
5.3 Tilgang til skjermingsverdige verdier hos byggherren	6
5.4 Avtale om håndtering og beskyttelse av ugradert skjermingsverdig informasjon og skjermingsverdig ugradert informasjonssystem	6
5.5 Krav til sikkerhetsavtale mellom byggherren og entreprenør, og eventuell leverandørklarering	6
5.6 Krav til autorisasjon, og eventuell sikkerhetsklarering av personell	6
6 INFORMASJON - PROFILERING	6
7 FILDELINGSPLATTFORM OG PROSJEKTHOTELL	6
VEDLEGG 1 – RAPPORTERING TIL OPPDRAGSGIVER	7
VEDLEGG 2 – ORIENTERING TIL LEVERANDØRER OM KRAV TIL HÅNDTERING OG BESKYTTELSE AV SKJERMINGSVERDIG INFORMASJON I FORBINDELSE MED ANSKAFFELSER	1



1 KVALITETSSIKRING

1.1 Generelt

Den prosjekterende skal i prosjektet ha implementert et system for kvalitetssikring for å sikre at arbeidene utføres i henhold til gjeldende forskrifter og kontraktens krav.

Den prosjekterende er ansvarlig for systematisk kontroll også av underleverandørers arbeider/leveranser som omfattes av kontrakten. Forsvarsbyggs kontraktspartner skal videreføre denne kontraktens krav til kvalitetssikring til sine kontraktspartnere nedover i kontraktspyramiden.

1.2 Kvalitetsplan

Det skal utarbeides en prosjektspesifikk kvalitetsplan, og det skal være tydelig kobling mellom kvalitetsplanen og prosjektspesifikke kontrollplaner og sjekklister. Kvalitetsplanen kan på relevante punkter henvise til den prosjekterendes kvalitetssystem, samt bygningsmyndighetenes krav. Kvalitetsplanen oversendes oppdragsgiver senest 4 uker etter kontraktsinngåelse.

1.3 Kontrollplaner og sjekklister

Den prosjekterende skal utarbeide prosjektspesifikke kontrollplaner for både rutinemessige og spesielle kvalitetskontroller som skal utføres for å verifisere at kontraktens krav, gjeldende offentligrettslige krav, samt kvalitetsplanen oppfylles.

Kontrollplanene 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)

Kontrollplanene og sjekklistene skal oversendes oppdragsgiver senest fire uker etter kontraktsinngåelse. Oppdragsgiver involvering skal fremkomme på prosjekterende sin kontrollplan ved at oppdragsgiver informerer om hvilke aktiviteter /sjekkpunkter det er ønskelig å delta på.

Verifikasjon skjer ved gjennomføring av kontroll i samsvar med kontrollplanene. Den prosjekterende skal dokumentere at kontroll er foretatt, og at resultatet er i samsvar med gitte krav. Avvik skal registreres og rapporteres.

Kontrollplanene skal holdes oppdatert i hele kontraktsperioden, og status rapporteres månedlig i månedsrapporten. På forespørsel skal oppdatert kontrollplan og sjekklister oversendes byggherren.

Dokumentasjon av kvalitetskontroll i form av registreringer (utfylte kontrollplaner med sjekklister / kontrollskjemaer) arkiveres hos den prosjekterende i hele bygge- og reklamasjonstiden, og tas inn i FDV-dokumentasjonen der dette er nødvendig.

1.4 Avviksbehandling

Den prosjekterende skal utrede konsekvensene av eventuelle avvik og rapportere forslag til behandling av avviket. Avvik skal medføre korrigerende tiltak for å hindre gjentakelse.



1.5 Revisjoner

Oppdragsgiver har rett til, etter en rimelig frist, å gjennomføre revisjon av den prosjekterendes oppfølging av kvalitetsplan og kontrollplan, herunder utførelse av kontraktsarbeidet, produksjonsprosessen, regnskap etc. Oppdragsgiver har også rett til å være tilstede ved interne og eksterne revisjoner som den prosjekterende selv gjennomfører overfor sine kontraktsmedhjelpere.

2 FREMDRIFTSTIDSPLANLEGGING, KOSTNADSSTYRING OG RAPPORTERING

2.1 Fremdriftsplan

Den prosjekterende skal senest fire uker etter kontraktsinngåelse utarbeide en fremdriftstidsplan som dekker kontraktarbeidet. Denne skal samordnes med oppdragsgivers hovedfremdriftsplan, og den skal være tydelig mht. hovedfrister, delfrister, kritiske aktiviteter, møter og avhengigheter. Fremdriftsplanen skal vise start- og sluttdato for alle aktiviteter. Fremdriftsplanen skal brytes ned til et nivå som sikrer en effektiv og kontrollerbar oppfølging. Det henvises til Del III A for beskrivelse av arbeidsmetodikk for detaljerte fremdriftsplaner ved hjelp av involverende planlegging.

2.2 Bemanningsplaner

Den prosjekterende skal senest fire uker etter kontraktsinngåelse etablere bemanningsplaner som viser planlagt og virkelig bemanning pr. fag og totalt for arbeidene.

2.3 Dokumentplan

Den prosjekterende skal utarbeide og vedlikeholde en dokumentplan som omfatter tekniske dokumenter og tegninger som den prosjekterende er ansvarlig for å utarbeide.

Dokumentplanen skal inneholde planlagte, virkelige og prognose datoer for viktige milepæler i dokumentproduksjonen. Dokumentplanen skal også inneholde opplysninger om hvilke dokumenter som skal oversendes oppdragsgiver for informasjon eller godkjenning.

Dokumentplanen skal være tilgjengelig for oppdragsgivers godkjenning senest fire uker etter kontraktsinngåelse.

2.4 Fremdriftsrapportering

Den prosjekterende skal rapportere fremdrift for arbeidene ved hjelp av frontlinje på fremdriftstidsplanen.

Det skal angis estimert timetall per aktivitet som skal benyttes som grunnlag for innbyrdes vektning av aktivitetene. Fremdriften skal rapporteres prosentvis pr. aktivitet og vises tabellarisk som planlagt og virkelig fremdrift. Rapportering av virkelig fremdrift skal gjøres ved en aggregering av virkelig fremdrift pr. dokument fra dokumentplanen.

Prosent fremdrift skal beregnes ut fra følgende metodikk:

$$\frac{100\% \times \text{virkelig forbrukte timer}}{\text{Forbrukte timer} + \text{estimerte gjenstående timeverk (sluttprognose)}}$$

Det skal utarbeides detaljerte fremdriftsplaner ved hjelp av involverende planlegging. Prosjekteringsgruppa skal gjennomføre interne korte statusmøter, såkalte tavlemøter for å rapportere på status på fremdriftsplanen, jmf. Kapittel XXX.

2.5 Krav til planleggingsverktøy

Fremdriftsplanen og detaljert fremdriftsplan skal leveres i et format som er kompatibelt med Microsoft Project. Detaljert fremdriftsplan kan fremstilles i annet verktøy etter avtale med byggherren.



FORSVARSBYGG

2.6 Faktureringsplan

Den prosjekterende skal utarbeide en tabellarisk faktureringsplan med måned som tidsenhet.

Faktureringsplanen danner ikke grunnlag for betaling av arbeidet. Arbeidet betales basert på utført produksjon.

2.7 Kostnadsrapportering

Den prosjekterende skal rapportere følgende nøkkeltall for kontraktstatus:

- Opprinnelig kontraktsverdi.
- Verdien av godkjente endringer.
- Verdien av omtvistede endringer
- Verdien av evt. endringsforespørsler under behandling.
- Planlagt og virkelig produksjon for perioden og akkumulert til statusdato
- Fakturert for perioden og akkumulert til statusdato.
- Produksjonsprognose for neste måned.

2.8 Rapporteringsperiode/statusdato (kutt dato)

Rapporteringsperiode er månedlig. Med mindre annet er avtalt, skal siste søndag i måneden være statusdato for innsamling av data for månedsrapporten.

2.9 Rapportering

I vedlegg 1 beskrives oppdragsgivers krav til tidsfrister og frekvens for rapportering.

Den prosjekterende innen 5 dager etter kutt dato, oversende en månedsrapport med følgende hovedpunkter:

- Kostnader
- Fremdrift
- Bemanning
- Kvalitet

I statusmøter med oppdragsgiver skal følgende faste poster inngå:

- Kostnader
- Fremdrift
- Bemanning
- Kvalitet

Oppdragsgiver skal ta referat fra slike statusmøter, dersom ikke annet er avtalt.

2.10 Endringsavtaler

Endringer skal formaliseres ved egne endringsavtaler før de iverksettes. Dette gjelder både når endringen har økonomiske og/eller fremdriftsmessige konsekvenser.

Byggherrens representant skal utstede/signere endringsavtalene.

3 FAKTURERING

3.1 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.

Ved fastprisoppdrag skal det sendes separate fakturaer for henholdsvis:

- Avdragsfakturaer



FORSVARSBYGG

- Endringsarbeider
- Lønns- og prisstigning
- Slutfaktura

Ved oppdrag honorert etter medgått tid skal det sendes separate fakturaer for henholdsvis:

- Medgåtte timer
- Slutfaktura

Se pkt 3.3 nedenfor for hvilke krav som stilles de ulike fakturakategoriene.

Forsvarsbyggs betalingsbetingelser er 28 dager etter mottak av faktura.

3.2 Krav til fakturaene

Alle fakturaer skal inneholde:

- Ressursnummer til attestant/mottaker <55157> oppgis under «Buyer reference».
- Prosjektnummer 100702, kontraktsnr. C03232 ». – oppgis i beskrivelsesfeltet.
- Faktura for endringsarbeider skal i beskrivelsesfeltet i tillegg henvise 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 den prosjekterende kunne få beskjed om at den umerkede/feilmerkede fakturaen ikke vil bli behandlet. Den prosjekterende plikter da å kreditere den umerkede fakturaen og utstede en ny korrekt faktura med ny fakturadato og nytt forfall.

3.3 Krav til de ulike fakturakategoriene

Avdragsfakturaer (for fastpriskontrakter):

Fakturaforsiden skal vise:

- Sum akkumulert produksjonsverdi.
- Sum akkumulert i flg. forrige avdragsfaktura.
- Totalbeløp i perioden (fakturabeløpet).

Faktura for arbeider som honoreres etter medgått tid, herunder for endringsarbeider

Attesterte timelister skal vedlegges fakturaene.

Lønns- og prisstigningsfakturaer (LPS).

Ved avtalt LPS skal det foretas beregning av dette etter samme periodisering som for avdragsfakturaer.

Beregningen skal fremkomme på LPS-fakturaene.

4 SPRÅK

Alle dokumenter, møtereferater mv. som skal framlegges på norsk, muntlige framstillinger og presentasjoner vil også foregå på norsk.

5 SIKKERHET

Gjennomføringen av kontrakten er ikke underlagt sikkerhetsrestriksjoner i henhold til sikkerhetslovens bestemmelser.

5.1 Prosjekterendes behov for tilganger til skjermingsverdige verdier

Byggherren har tatt stilling til hva prosjekterende kan få tilgang til av skjermingsverdig informasjon, informasjonssystemer, objekter eller infrastruktur (skjermingsverdige verdier).



FORSVARSBYGG

Prosjekterende har kun behov for tilgang til skjermingsverdige verdier hos oppdragsgiveren.

Krav til beskyttelse av skjermingsverdig informasjon er gitt i vedlegg 2.

For beskyttelse av skjermingsverdig informasjon som er ugradert, se vedlegg 2 punkt 1 og 2.

5.2 Tilgang til skjermingsverdig informasjon i prosjekterendeens egne lokaler

Entreprenøren vil ikke ha behov for å oppbevare eller behandle informasjon i papirform som er skjermingsverdig. Prosjekterende vil ikke ha behov for å behandle informasjon på informasjonssystem som er skjermingsverdig. Informasjonssystem hos entreprenør som skal behandle skjermingsverdig informasjon skal godkjennes før det tas i bruk.

Informasjonssystem hos prosjekterende vil ikke være tilknyttet skjermingsverdig objekt eller infrastruktur.

5.3 Tilgang til skjermingsverdige verdier hos byggherren

Prosjekterende vil ha behov for tilgang til skjermingsverdig informasjon (i papirform eller elektronisk) hos byggherren under oppsyn av representant for byggherren. Informasjonen vil være skjermingsverdig ugradert.

Prosjekterende vil ha behov for fysisk tilgang til skjermingsverdig objekt eller infrastruktur under oppsyn av representant for byggherren. Objektet eller infrastrukturen vil være klassifisert VIKTIG.

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

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

For denne kontrakten gis det tilgang til ugradert skjermingsverdig informasjon.

5.5 Krav til sikkerhetsavtale mellom byggherren og entreprenør, og eventuell leverandørklarering

Før prosjekterende gis tilgang til skjermingsverdige verdier er det ingen krav til sikkerhetsavtale eller leverandørklarering.

5.6 Krav til autorisasjon, og eventuell sikkerhetsklarering av personell

Før prosjekterendes personell gis tilgang til skjermingsverdige verdier er det krav til autorisasjon for informasjon sikkerhetsgradert BEGRENSET.

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

6 INFORMASJON - PROFILERING

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

Dersom den prosjekterende eller noen av den prosjekterendes kontraktsmedhjelpere for reklameformål eller annen måte ønsker å gi offentligheten informasjon om oppdraget, skal dette alltid forelegges oppdragsgiveren på forhånd til godkjenning.

7 FILDELINGSPLATTFORM OG PROSJEKTHOTELL

Forsvarsbygg har en fildelingsplattform for deling av informasjon. <http://joint.prosjekthotell.com/eroom/> med påloggingsnavn raadgivende@forsvarsbygg.no, passord: Ingeniør1



Prosjektet vil bruke prosjekthotell Interaxo for dokumenthåndtering og informasjonsdeling.

Vedlegg 1 – Rapportering til oppdragsgiver

I forbindelse med kontraktsinngåelse / oppstart av arbeidene:

Leveranse	Ref.	Fremdriftsplan / frekvens
Prosjektspesifikk kvalitetsplan	Del III-D pkt. 1.2	4 uker etter kontraktsinngåelse.
Kontrollplaner for kvalitetssikring	Del III-D pkt. 1.3	4 uker etter kontraktsinngåelse.
Fremdriftsplan	Del III-D pkt. 2.1	4 uker etter kontraktsinngåelse.
Bemanningsplan	Del III-D pkt. 2.2	4 uker etter kontraktsinngåelse.
Faktureringsplan	Del III-D pkt. 2.6	4 uker etter kontraktsinngåelse.

Periodisk rapportering:

Leveranse	Ref.	Tidsfrist / frekvens
Kontrollplaner for kvalitetssikring	Del III-D pkt. 1.3	Se del III-D pkt 2.9
Fremdriftsplan	Del III-D pkt. 2.1	Se del III-D pkt 2.9
Bemanningsplan	Del III-D pkt. 2.2	Se del III-D pkt 2.9
Faktureringsplan	Del III-D pkt. 2.6	Se del III-D pkt 2.9

I forbindelse med avslutning av arbeidene:

Leveranse	Ref.	Tidsfrist / frekvens
Risikovurdering iht. byggherreforskriften	Del III-E1	

Vedlegg 2 – 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 terrorhandling, 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 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.

4.2.2. 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 skjermingsverdige 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 skjermingsverdige 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 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. Godkjenning av skjermingsverdige informasjonssystem

NSM er godkjenningmyndighet 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 skjermingsverdige informasjonssystemer. Ved å følge NSMs og Forsvarsbyggs veiledere for godkjenning av informasjonssystemer anses kravene § 49 som ivarettatt.

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

Tempestrisikovurdering må utarbeides i tillegg til dokumentasjonen som er aktuell for skjermingsverdige 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 skjermingsverdige objekt eller skjermingsverdige 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/>.

