



## KONKURRANSEGRUNNLAGETS DEL III - NS 8406

### Oppdraget

#### INNHold

<b>1 INNLEDNING</b>	<b>3</b>
<b>2 ORIENTERING OM OPPDRAGET (KONTRAKTEN)</b>	<b>3</b>
2.1 Entrepriseform	3
2.2 Byggherrens organisasjon	3
2.3 Nærmere om bygge- og anleggsarbeidet	3
2.3.1 Beskrivelse av de aktuelle bygge- og anleggsarbeidene	3
2.3.2 Beskrivelse av opsjoner	3
2.3.3 Tomteforhold	3
2.3.4 Status i forhold til offentlige myndigheter	Feil! Bokmerke er ikke definert.
2.3.5 Orientering om spesielle forhold	3
2.4 Hovedaktiviteter i denne kontrakten	4
2.4.1 Rigg og drift	4
2.4.2 Bygningsmessige arbeider	4
2.4.3 VVS-arbeider	4
2.4.4 Elektroarbeider	4
2.4.5 Tele-/dataarbeider	Feil! Bokmerke er ikke definert.
2.4.6 Andre installasjoner (heisarbeider)	Feil! Bokmerke er ikke definert.
2.4.7 Utenomhusarbeider	Feil! Bokmerke er ikke definert.
2.5 Grensesnitt mot andre aktører	Feil! Bokmerke er ikke definert.
2.6 Tiltransport og byggeplassadministrasjon	4
2.6.1 Tiltransport til underentreprise	4
2.6.2 Byggeplassadministrasjon med fremdriftskontroll av entreprenør	4
2.7 Mengdekontroll	4
2.8 Overføring av risiko for utført prosjektering – Entreprenørens plikt til å utføre nødvendig/gjenstående prosjektering	4
2.9 Prøvedrift	4
2.10 Lærlingklausul	4
<b>3 FREMDRIFT OG TIDSFRISTER</b>	<b>4</b>
<b>4 SIKKERHET, HELSE OG ARBEIDSMILJØ (SHA)</b>	<b>5</b>
4.1 Prosjekter omfattet av byggherreforskriften	5
4.2 Sikring av og på byggeplassen	5
4.3 Føring av oversiktslister	5
4.4 HMS-kort	6
4.5 Opplæring	6
4.6 Språkkrav	6
4.7 Verneutstyr	7
<b>5 YTRE MILJØ</b>	<b>7</b>
5.1 Ansvar og myndighet	7
5.1.1 Prosjektering	7
5.1.2 Gjennomføring	7
<b>6 FDVU-DOKUMENTASJON</b>	<b>7</b>
<b>7 KVALITET</b>	<b>8</b>
7.1 Kvalitetsplan	Feil! Bokmerke er ikke definert.
7.2 Kontrollplan	Feil! Bokmerke er ikke definert.
<b>8 FREMDRIFTSSTYRING</b>	<b>8</b>

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

8.1 Fremdriftsplan .....	8
8.2 Krav til format på fremdriftsplan.....	8
<b>9 MØTER .....</b>	<b>8</b>
<b>10 FAKTURERING (NS 8406 PUNKT 23).....</b>	<b>9</b>
10.1 Generelle faktureringsbestemmelser.....	9
10.2 Avdragsfaktura .....	9
10.3 Faktura for endringsarbeider .....	9
10.4 Lønns- og prisendringer .....	<b>Feil! Bokmerke er ikke definert.</b>
10.5 Sluttfaktura .....	9
10.6 Krav til merking.....	9
<b>11 KORRESPONDANSE.....</b>	<b>9</b>
<b>12 INFORMASJON – PROFILERING .....</b>	<b>10</b>
<b>13 SIKKERHET .....</b>	<b>10</b>
13.1 Entreprenørens behov for tilgang til skjermingsverdige verdier.....	<b>Feil! Bokmerke er ikke definert.</b>
13.2 Tilgang til skjermingsverdige informasjon i entreprenørens egne lokaler .....	10
13.3 Tilgang til skjermingsverdige verdier hos byggherren .....	<b>Feil! Bokmerke er ikke definert.</b>
13.4 Avtale om håndtering og beskyttelse av ugradert skjermingsverdige informasjon og skjermingsverdige ugradert informasjonssystem .....	<b>Feil! Bokmerke er ikke definert.</b>
13.5 Krav til sikkerhetsavtale mellom byggherren og entreprenør, og eventuell leverandørklarering	<b>Feil! Bokmerke er ikke definert.</b>
13.6 Krav til autorisasjon, og eventuell sikkerhetsklarering av personell .....	<b>Feil! Bokmerke er ikke definert.</b>
<b>VEDLEGG 1 – OVERSIKT OVER FRISTER FOR FREMLEGGELSE AV DOKUMENTER OG RAPPORTERING.....</b>	<b>10</b>
<b>VEDLEGG 2 – ORIENTERING TIL LEVERANDØRER OM KRAV TIL HÅNDTERING OG BESKYTTELSE AV SKJERMINGSVERDIG INFORMASJON I FORBINDELSE MED ANSKAFFELSER.....</b>	<b>1</b>

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

## 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](http://www.forsvarsbygg.no).

Forsvaret trenger flere boliger til sine ansatte. Forsvarsbygg ønsker på denne bakgrunn tilbud på renovering av leiligheter slik at de blir attraktive å bo i.

## 2 ORIENTERING OM OPPDRAGET (KONTRAKTEN)

### 2.1 Entrepriseform

Denne kontrakten gjennomføres som en entreprise basert på NS 8406.

Merk at punkt 2.7 regulerer om prosjektering er inkludert.

### 2.2 Byggherrens organisasjon

Byggherrens organisasjon inkludert prosjekteringsytelser er organisert slik:

Funksjon	Firma	Kontaktperson
Prosjektleder	Forsvarsbygg	Knut Wikstrøm
Byggeleder/KP/KU	PPM Prosjekt	Torleiv Hov Grønbech
SHA-rådgiver	Forsvarsbygg	Eirik Fonnum

### 2.3 Nærmere om bygge- og anleggsarbeidet

#### 2.3.1 Beskrivelse av de aktuelle bygge- og anleggsarbeidene

Det skal renoveres leiligheter i Arthur Nordlies vei. I utgangspunktet skal 17 leiligheter renoveres, men dette avhenger av finansiering.

#### 2.3.2 Beskrivelse av opsjoner

Oppdragsgiver har opsjon på renovering av flere leiligheter, delt opp etter leilighetstype. Fristforlengelse vil vurderes når utløsning av opsjon eventuelt skjer.

#### 2.3.3 Tomteforhold

Arbeidene vil foregå i et sameie med grøntarealer og lekeplasser. Riggplass og ferdsel på tomten avtales med sameiet og må hensyntas fra entreprenør.

#### 2.3.4 Orientering om spesielle forhold

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

## 2.4 Hovedaktiviteter i denne kontrakten

### 2.4.1 Rigg og drift

### 2.4.2 Bygningsmessige arbeider

### 2.4.3 VVS-arbeider

### 2.4.4 Elektroarbeider

## 2.5 Tiltransport og byggeplassadministrasjon

### 2.5.1 Tiltransport til underentreprise

- ☐ Alternativ 1: Entreprenøren kan få tiltransportert sideentreprenører som blir hans underentreprenører.
- ☐ Alternativ 2: Entreprenøren kan tiltransporteres til en sideentreprenør
- ☒ Alternativ 3: Tiltransport er ikke avtalt.

Er det ikke krysset av for noen av alternativene, gjelder alternativ 1.

### 2.5.2 Byggplassadministrasjon med fremdriftskontroll av entreprenør

- ☒ Alternativ 1: Entreprenøren kan underlegges byggplassadministrasjon og fremdriftskontroll eller pålegges å utføre byggplassadministrasjon og fremdriftskontroll av sideentreprenører.
- ☐ Alternativ 2: Byggplassadministrasjon er ikke avtalt.
- ☐ Alternativ 3: Entreprenøren kan underlegges byggplassadministrasjon og fremdriftskontroll.

Er det ikke krysset av for noen av alternativene, gjelder alternativ 1.

## 2.6 Mengdekontroll

Entreprenøren skal ikke foreta mengdekontroll.

## 2.7 Overføring av risiko for utført prosjektering – Entreprenørens plikt til å utføre nødvendig/gjenstående prosjektering

Entreprenøren har risikoen for løsninger og annen prosjektering som måtte følge av byggherrens oppdragsbeskrivelse for kontraktsinngåelsen. Entreprenøren skal i tillegg utføre all nødvendig/gjenstående detaljprosjektering som oppdraget krever.

## 2.8 Prøvedrift

Det skal ikke gjennomføres prøvedriftperiode.

## 2.9 Lærlingklausul

Ved utførelsen av kontraktsarbeidet skal minimum 10 % av arbeidede timer innenfor bygg- og anleggsgagnene samlet (de fag som omfattes av utdanningsprogrammet for bygg- og anleggsteknikk, samt anleggsgartnerfaget) utføres av lærlinger, jf. opplæringslova §§ 3-5 og 4-1.

## 3 FREMDRIFT OG TIDSFRISTER

Forsvarsbygg har satt følgende tidsplan for gjennomføringen av oppdraget. Forsvarsbygg kan kreve dagmulkt i henhold til kontraktsbestemmelsene for overskridelse av de oppgitte dagmulktbelagte fristene.

Nr.	Beskrivelse	Dato	Dagmulkt
1	Kontraktsinngåelse	01.07.26	Nei

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

2	Fremleggelse av detaljert fremdriftsplan med støyplan	To uker etter kontraktsinngåelse	Ja
3	Igangsetting av arbeid på byggeplass	03.08.2026	Ja
4	Levering av FDVU-dokumentasjon	05.11.26	Ja
5	Overtakelse av kontraktarbeidet	26.11.26 eller annen avtalt dato, ref. Del I pkt. 5.3.3.	Ja

Tidsplan for utsendelse av byggherrens arbeidstegninger gjennomgås i forbindelse med kontraktsinngåelsen, sett i lys av entreprenørens planlagte framdrift.

#### 4 Sikkerhet, helse og arbeidsmiljø (SHA)

Forsvarsbygg har en nullvisjon og mål om å unngå alle skader og farlige tilfeller i prosjekter. Det forventes høy standard på SHA-arbeidet og godt samarbeid mellom alle involverte virksomheter.

For alle arbeidere skal hver enkelt entreprenør gjennomføre ukentlige vernerunder innenfor sin kontrakt. Alle vernerunder skal rapporteres skriftlig og følges opp.

Entreprenøren skal umiddelbart rapportere alle skader og alvorlige hendelser muntlig eller skriftlig til byggherre. Ved muntlig varsling skal denne følges opp skriftlig samme dag som hendelsen, så snart dette er praktisk mulig. Skjema med foreløpige tiltak skal være hos byggherre innen 24 timer etter hendelsen.

Endelig granskning med kartlegging av årsaker og tiltak skal leveres byggherre innen 14 dager om ikke annet er avtalt.

##### 4.1 Prosjekter omfattet av byggherreforskriften

For arbeidere som er omfattet av byggherreforskriften skal entreprenøren:

- iverksette Forsvarsbyggs prosjektspesifikke SHA-plan, og informere byggherren om forhold som ikke er beskrevet i planen.
- videreføre SHA-planen for gjennomføringsfasen
- integrere Forsvarsbyggs SHA-krav som en del av entreprenørens egne systemer
- sørge for at Forsvarsbyggs SHA-krav videreføres i kontrakter til underentreprenører.
- sørge for at forebyggende tiltak innføres.

##### 4.2 Sikring av og på byggeplassen

Entreprenøren skal om nødvendig sikre bygg-/riggplassen med godkjent gjerde. Sikringen skal være tilpasset den enkelte lokasjon og ivareta ytre miljø.

##### 4.3 Førings av oversiktslister

Entreprenøren skal benytte byggherrens system for registrering og oppfølging av entreprenører – HMS-reg.

#### Beskrivelse alternativ 1: Entreprenøren skal benytte byggherrens system for registrering og oppfølging av entreprenører.

Kortlesersystemet som skal benyttes i prosjektet skal overføre relevante data til byggherrens system for registrering og oppfølging av entreprenører.

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

Entreprenøren skal benytte byggherrens system for registrering og oppfølging av entreprenører for seg og sine underentreprenører. Det innebærer som minimum følgende administrative oppgaver:

- registrere egne ansatte.
- registrere underentreprenører.
- gi underentreprenørene tilgang til å registrere sine underentreprenører og egne ansatte.
- oppdatere informasjon om underentreprenører og arbeidstakere ved endringer.
- følge opp at alt personell i leverandørkjeden registrerer seg inn og ut på bygge- og anleggsplass, blant annet ved tilstedekontroller i systemet.
- laste opp påkrevde dokumenter i systemet.
- følge opp at etterspurt dokumentasjon blir levert innen gitt frist ved seriositetskontroller i systemet.
- lukke avvik som byggherren avdekker ved seriositetskontroller i systemet innen angitt frist.

Ved registrering av personell i byggherrens system for registrering og oppfølging av entreprenører må telefonnummer alltid oppgis.

#### Tekniske krav

Kortlesersystemet skal kunne lese av HMS-kort og kunne levere passeringsdata, og som et minimum skal passeringsinformasjonen inneholde:

- HMS-kortnummer
- Passeringstidspunkt (klokkeslett)
- Passeringsretning (inn/ut)

Informasjonen skal leveres via API på en måte slik at informasjonen kan overføres løpende til byggherrens system for registrering og oppfølging av entreprenører.

#### Krav til informasjonssikkerhet (i adgangskontrollsystemet til entreprenøren)

Entreprenør med ansvar for å levere, montere og drifte kortlesersystemet er ansvarlig for at informasjonssikkerheten i kortlesersystemet på byggeplassen er tilfredsstillende ivaretatt både for seg og sine underentreprenører.

### **4.4 HMS-kort**

Alle arbeidstakere skal, lett synlig, bære gyldig HMS-kort utstedt av Arbeidstilsynet. Ordrebekreftelse, søknadsskjema og aksepteres ikke som HMS-kort. Arbeidstakere som ikke har slikt HMS-kort vil bli bortvist fra byggeplassen.

### **4.5 Opplæring**

Entreprenøren skal sikre at alle utførende deltar på hovedbedrifts HMS-introduksjon og at personlig sikkerhetsinstruks (PSI) fylles ut og signeres før oppstart på byggeplass. For å sikre at alle som skal arbeide på byggeplassen gjennomgår opplæringen, skal entreprenøren planlegge, og gjennomføre HMS-kurs på byggeplassen. Alle på byggeplassen skal delta på opplæringen. Byggherrens representanter skal gis mulighet til å delta på HMS-kursene.

Entreprenøren skal føre oversikt over og rapportere månedlig hvem som har gjennomført denne opplæringen. Byggherrens SHA-plan skal inngå i HMS-opplæringen.

Alle som skal utføre arbeid på bygge- og anleggsplass skal ha gjennomført e-læringskurset Prosjekt Fareblind og Farlige mønstre (begge tilgjengelig via [www.sfsba.no](http://www.sfsba.no)). Alle skal til enhver tid ha gyldig kursbevis. Bekreftelse på gjennomført kurs skal kunne fremvises på forespørsel.

### **4.6 Språkkrav**

Med mindre annet er avtalt, skal all kommunikasjon mellom nøkkelpersoner i prosjektet foregå på norsk.

Entreprenøren skal sørge for at egne arbeidstakere og eventuelle underentreprenører kan kommunisere på en slik måte at manglende kommunikasjon ikke utgjør en sikkerhetsrisiko. For å unngå at det skjer ulykker fordi ikke alle forstår informasjonen som blir gitt, gjelder følgende:

- Minst én av det utførende personell på ethvert arbeidslag skal kunne forstå og gjøre seg forstått på norsk eller engelsk. Dersom flere utfører oppdrag sammen, skal vedkommende i tillegg forstå og gjøre seg forstått på et språk alle de andre på arbeidslaget forstår og kan gjøre seg forstått på.
- Alle på byggeplassen skal forstå SHA-plan, sikkerhetsopplæring, HMS-rutiner, verneprotokoller, sikkerhetsinstrukser, SJA, sikkerhetsdatablader, bruksanvisning for verktøy og arbeidsutstyr, varselskilter mv. Materialet skal foreligge på det språk vedkommende arbeidstaker bruker som morsmål, såfremt arbeidstakeren ikke forstår informasjonen fullt ut på norsk eller engelsk.

#### 4.7 Verneutstyr

Følgende verneutstyr skal alltid benyttes på byggeplassen:

- Synlighetstøy på overkropp (min. klasse 2)
- Hjelm
- Vernesko/støvler (sandaler og sko uten hæl aksepteres ikke).

Arbeidsgiver skal stille alt nødvendig verneutstyr, basert på aktivitet, tilgjengelig.

### 5 YTRE MILJØ

#### 5.1 Ansvar og myndighet

##### 5.1.1 Prosjektering

Dersom entreprenøren skal prosjektere (jfr. punkt 2.8) skal entreprenøren:

- a) foreta nødvendige risikovurderinger ved oppstart og gjennom hele prosjekteringen. Restrisiko, inkl. hvilke risikoer som krever spesifikke tiltak, skal beskrives.

##### 5.1.2 Gjennomføring

Entreprenøren skal:

- a) integrere byggherrens krav til Ytre Miljø som en del av entreprenørens egne systemer
- b) sørge for at byggherrens miljøkrav videreføres i kontrakter til underentreprenører

### 6 FDVU-dokumentasjon

Entreprenør plikter å følge krav om forsvarlig FDVU-dokumentasjon i henhold til reguleringer i plan og bygningsloven og detaljert beskrivelse av hva som skal leveres er beskrevet i NS/TS 3456:2018. Ved oppdateringer i lov eller standard skal entreprenør forholde seg til oppdatert versjon. Jf. Del III C1 FDVU.

Før overlevering foretas en gjennomgang av materialet med prosjektleder. Forsvarsbygg kontrollerer dokumentasjonens navngivning og struktur og legger den inn i respektive systemer for lagring.

All FDVU-dokumentasjon skal ha filnavn som er selvforklarende. Dokumenter skal navnes slik at de er gjenfinnbare på bygningsdel og/eller fritekst, se eksempel nedenfor.

Filnavnet skal alltid starte på bygningsdelsnummeret, primært på tresifret nivå. Der filen inneholder informasjon som gjelder flere bygningsdeler navnes, og leveres, filen på det som naturlig må anses som «hovednummer». TFM-kode kan benyttes som filnavn.

Filnavnet må holdes kort og bør ikke overskride 20 tegn. Tegninger og bygningsmodeller skal alltid leveres i proprietært format. (Originalformat) i tillegg til pdf.

Eksempler:

244 Prod.db dør Jømna EM-200

442 Armaturlister med plassering

442 Armaturtyper dokumentasjon

453 Prod.db varmekabel bebehold water pipe

365 EC-vifte MXPC63RD-1450

## 7 Kvalitet

Entreprenøren skal ha et implementert og dokumentert system for å sikre at arbeidene utføres i henhold til gjeldende lover, forskrifter, kontraktens krav og eventuelt entreprenørens egne krav.

Entreprenøren skal holde kvalitetssystem løpende oppdatert og komplett. På forespørsel skal oppdatert kvalitetsoversikt oversendes byggherren. Entreprenøren er ansvarlig for at relevante deler kvalitetsplanen er kjent for alle underleverandører.

## 8 Fremdriftsstyring

Entreprenøren skal ivareta en forsvarlig planlegging, styring, koordinering og kontroll av fremdrift for å sikre at kontraktens tidsfrister overholdes. Entreprenøren skal herunder sikre tilstrekkelig bemanning, og ivareta krav til sikkerhet, helse og arbeidsmiljø på bygge- og anleggsplassen.

### 8.1 Fremdriftsplan

Entreprenøren skal senest to uker etter kontraktsinngåelsen utarbeide og fremlegge en fremdriftsplan for kontraksarbeidet. Fremdriftsplanen skal være basert på byggherrens tidsplan og skal synliggjøre alle aktiviteter og faser som omfattes av kontrakten. SJA skal synliggjøres som egne aktiviteter i fremdriftsplanen. For hver aktivitet skal planen vise (*angitt ved kryss*):

- ☒ Aktivitetskode og –beskrivelse
- ☒ Viktige milepeler (dagmukltbelagte milepeler, milepeler som tett hus, byggherrebeslutninger mv.)
- ☒ Planlagt start- og sluttdato
- ☒ Avhengigheter mellom aktiviteter i prosjekter (f.eks. ytelser fra byggherren, sideentreprenører eller øvrige aktører i prosjektet)
- ☒ Kritisk linje
- ☐ Timeverk

Fremdriftsplanen skal normalt detaljeres pr. kontrollareal ned til tre- til femsifret nivå i henhold til Norsk Standards bygningsdelstabell (NS 3451:2009). Kontrollareal fastsettes i samråd med byggherren. Planen justeres i nødvendig omfang i tråd med kontraktens regler om samordning.

### 8.2 Krav til format på fremdriftsplan

Fremdriftsplanen og detaljert fremdriftsplan skal leveres i et format som er kompatibelt med Microsoft Project.

## 9 Møter

Entreprenøren skal delta i de møter byggherren innkaller til. Normalt gjennomføres byggemøter hver andre uke. Hvis partene ikke blir enige om annet er byggherren ansvarlig for å skrive referat fra møtene. Det etableres en fast agenda for møtene. Byggherren kan kreve at entreprenøren gir en kort skriftlig oppsummering av status knyttet til hovedpunktene i agendaen i forkant av hvert møte.

Entreprenøren holder møter med sine kontraktsmedhjelpere i nødvendig utstrekning. Med mindre annet blir bestemt, skal prosjekteringsmøter og underentreprenørmøter holdes hver annen uke. Byggherren skal motta innkalling, og har rett til å delta i møtene. Referat fra møtene skal føres av entreprenøren. Byggherren skal motta kopi av møtereferatet.



## 10 Fakturering (NS 8406 punkt 23)

### 10.1 Generelle faktureringsbestemmelser

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](http://www.ehandel.no).

Entreprenøren skal sende separate fakturaer for:

- Kontraktssum (avdragsfaktura)
- Godkjente endrings- og tilleggsarbeid
- Slutfaktura

Forsvarsbyggs betalingsfrist er 28 dager etter mottak av faktura (gjelder ikke slutfaktura).

### 10.2 Avdragsfaktura

Avdrag på kontraktssummen skal faktureres månedlig. Det skal trekkes innestående beløp. Restbeløpet utgjør fakturabeløpet, ink. merverdiavgift.

Når fakturaen omfatter regulerbare poster skal fakturaen ha et vedlegg som viser beregning av vederlag basert på kontraktens enhetspriser og utførte mengder pr. avregningsdato. Oppsettet skal følge mengdebeskrivelsen og inneholde de samme postene som denne. Avholdte målinger vedlegges som dokumentasjon for utført volum. Vederlag etter medgått tid eller etter regning skal dokumenteres ved spesifiserte timelister, fakturaer over innkjøpt materiell mv.

Byggherren kan i rimelig utstrekning kreve ytterligere dokumentasjon.

### 10.3 Faktura for endringsarbeider

Faktura for endringsarbeider faktureres i egen faktura når arbeidet er ferdigstilt. Ved endringsarbeider av lengre varighet kan entreprenøren kreve avdrag på grunnlag av det som er utført, men ikke oftere enn hver måned. Fakturering skal skje separat for hver enkelt endringsavtale.

Fakturaen skal spesifiseres og vedlegges den dokumentasjon som er nødvendig for byggherrens kontroll.

### 10.4 Slutfaktura

Entreprenøren skal sende slutfaktura med sluttoppstilling i samsvar med kontraktens bestemmelser, jf. NS 8406 punkt 25.1.

### 10.5 Krav til merking

Alle fakturaer skal inneholde:

- Ressursnummer til attestant 57881 oppgis under «Buyer reference».
- «Prosjektnummer 101443, kontraktsnr. C06570». – oppgis i beskrivelsesfelt.
- Faktura for endringsarbeider skal i beskrivelsesfeltet i tillegg henvise til endringsavtalenummer (E001, E002 osv.).

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

## 11 Korrespondanse

Formell korrespondanse mellom partene skal merkes med prosjektnummer/-navn og kontraktsnummer. Deretter angis hva saken gjelder.

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

Her skal det stå:

F.eks. 101443 – Arthur Nordlies Vei – C06570 - Oversendelse av referat

Det skal fremgå av korrespondansen hvem som er kopimottaker(e).

## 12 Informasjon – profilering

All kontakt med media og publikum skal håndteres av byggherren. Henvendelser fra media, eller forespørsler om innsyn, skal henvises til byggherrens prosjektleder eller annen oppgitt kontaktperson for slike henvendelser. Dersom entreprenøren eller noen av entreprenørens kontraktsmedhjelpere for reklameformål eller annen måte ønsker å gi offentligheten informasjon om oppdraget, skal dette alltid forelegges byggherren på forhånd til godkjennelse.

## 13 Sikkerhet

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

### 13.1 Tilgang til skjermingsverdig informasjon i entreprenørens egne lokaler

Entreprenøren vil ikke ha behov for å oppbevare eller behandle informasjon i papirform som er skjermingsverdig. Entreprenøren vil ikke ha behov for å behandle informasjon på informasjonssystem som er skjermingsverdig. Informasjonssystem hos entreprenøren vil ikke være tilknyttet skjermingsverdig objekt eller infrastruktur.

## Vedlegg 1 – Oversikt over frister for fremleggelse av dokumenter og rapportering

Dokumenter som skal fremlegges i forbindelse med kontraktsinngåelse/oppstart av arbeidene:		Sett kryss
Dokument:	Frist	
Medlemsbevis fra Grønt Punkt Norge eller tilsvarende ordning	Ved kontraktsinngåelse	
Miljøstyringssystem – sertifikat eller annen dokumentasjon	14 dager etter kontraktsinngåelse	
Helse- og miljøfarlige stoffer og produkter	14 dager etter kontraktsinngåelse	
Garantierklæring	14 dager etter kontraktsinngåelse	
Kvalitetsplan	På forespørsel	
Fremdriftsplan (detaljert)	2 uker etter kontraktsinngåelse	
Dokumenter som skal fremlegges i forbindelse med avslutning av arbeidene:		Sett kryss
FDVU-dokumentasjon og annet sluttokumentasjon	3 uker før overtakelse	

Periodiske rapporter:		
Tema:	Metode:	Frekvens:
<b>Kvalitet</b> <ul style="list-style-type: none"> <li>Kvalitetsrapport, overordnet om evt. +/-</li> </ul>	Byggemøter	Hver 14. dag
<b>Fremdrift</b> <ul style="list-style-type: none"> <li>Fremdriftsplan med oppdatert fremdriftsfront</li> </ul>	Byggemøter	Hver 14. dag

Prosjektnr:

Prosjektets navn:

Kontraktsnr:

<b>Bemanning</b> <ul style="list-style-type: none"><li>Bemanning</li></ul>	Byggemøter	Hver 14. dag
<b>Produksjon</b> <ul style="list-style-type: none"><li>Produksjon for perioden og akkumulert til statusdato</li><li>Fakturert for perioden og akkumulert til statusdato</li><li>Produksjonsprognose for neste måned</li></ul>	Byggemøter	Hver 14. dag
<b>SHA</b> <ul style="list-style-type: none"><li>Mannskap- og timeforbruk</li><li>Uønskede hendelser i perioden</li><li>Vernerunder</li><li>Sikker jobb-analyser (SJA) mv.</li></ul>	Byggemøter	Hver 14. dag
<b>Miljø</b> <ul style="list-style-type: none"><li>Bruk av helse- og miljøfarlige stoffer</li><li>Avfall</li></ul>	Byggemøter	Hver 14. dag

## Vedlegg 2 – Orientering til leverandører om krav til håndtering og beskyttelse av sikkerhetsgradert informasjon i leverandørens egne lokaler

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

## 1. Innledning

### 1.1. Formål

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

### 1.2. Definisjoner

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

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

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

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

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

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

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

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

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

### 1.3. Sikkerhet i anskaffelser

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

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

## 1.4. Hjemmel

### 1.4.1. Sikkerhetsloven med forskrifter

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

Sentrale forskrifter som er hjemlet i sikkerhetsloven:

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

### 1.4.2. Forholdet til regelverket om offentlige anskaffelser

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

## 1.5. Generelle krav til forebyggende sikkerhetsarbeid

### 1.5.1. Styringssystem for sikkerhet

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

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

### 1.5.2. Leverandørens ansvar

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

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

### 1.5.3. Krav om forsvarlig sikkerhetsnivå

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

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

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

NSM har publisert veiledere som gir anbefalinger om hvordan lov og forskrifter er å forstå, og danner et grunnlag for virksomhetenes arbeid med å etterleve regelverket. NSM har i tillegg publisert håndbøker og tekniske råd som gir mer utfyllende anbefalinger om hvordan lovens funksjonelle krav kan oppfylles. Håndbøkene og de tekniske rådene beskriver fremgangsmåter, prosedyrer og gir eksempler på tiltak for å hjelpe virksomhetene i regelverksanvendelsen, se [www.nsm.no](http://www.nsm.no).

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



#### 1.5.4. Utgifter til oppfyllelse av sikkerhetskrav

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

#### 1.5.5. Brudd på sikkerhetskrav

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

## 2. Sikkerhetsgraderte anskaffelser på BEGRENSET nivå

### 2.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert BEGRENSET

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

### 2.2. Inngåelse av sikkerhetsavtale på BEGRENSET nivå

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

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

Følgende dokumenter må utarbeides av leverandøren og sendes til oppdragsgiver:

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

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

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

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

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

### 2.2.1. Autorisasjon

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

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

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

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

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

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

### 2.2.2. Autorisasjon av utenlandsk statsborger

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

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



### 2.2.3. Godkjenning av skjermingsverdig informasjonssystem

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

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

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

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

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

Oppdragsgiver har maler for hver av de ovennevnte dokumenter.

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

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

### 2.2.4. Unntak fra krav om sikkerhetsavtale

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

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

### 2.2.5. Brudd på sikkerhetskrav

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

### 3. Sikkerhetsgraderte anskaffelser på KONFIDENSIELT nivå

#### 3.1. Forsvarlig sikkerhetsnivå for informasjon som er gradert KONFIDENSIELT

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

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

##### 3.1.1. Soneinndeling for informasjon gradert KONFIDENSIELT

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

##### 3.1.2. Godkjenning av skjermingsverdig informasjonssystem

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

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

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

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

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

##### 3.1.3. Leverandørklarering

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

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

##### 3.1.4. Sikkerhetsklarering og autorisasjon av leverandørpersonell

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

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

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

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

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

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

#### *3.1.5. Sikkerhetsklarering og autorisasjon av leverandørpersonell med utenlandsk statsborgerskap*

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

### **3.2. Inngåelse av sikkerhetsavtale på KONFIDENSIELT nivå**

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

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

#### *3.2.1. Brudd på sikkerhetskrav*

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