

Bilag 4 – Informationssikkerhed

Indholdsfortegnelse

Definitioner og referencer	4
1. Generelle krav til cyber- og informationssikkerhed	5
2. Informationssikkerhedspolitikker	5
2.1. Styringsgrundlag for informationssikkerhed	5
3. Organisering af informationssikkerhed	5
3.1. Intern Organisering	5
3.2. Mobilt Udstyr	6
4. Personalesikkerhed	6
4.1. Under ansættelsen	6
4.2. Ansættelsesforholdets ophør eller ændring	7
5. Styring af aktiver	7
5.1. Ansvar for aktiver	7
5.2. Mærkning af informationer	8
5.3. Mediehåndtering	8
6. Adgangsstyring	9
6.1. Forretningsmæssige krav til adgangsstyring	9
6.2. Tildeling og administration af brugeradgang	9
6.3. Brugernes ansvar	10
6.4. Styring af system- og applikationsadgang	11
7. Kryptografi	12
7.1. Kryptografiske kontroller	12
8. Fysisk sikring og miljøsikring	12
8.1. Sikre områder	12
8.2. It-Udstyr	12
9. Driftssikkerhed	13
9.1. Driftsprocedurer og ansvarsområder	13
9.2. Beskyttelse mod malware	13
9.3. Backup	13
9.4. Logning og overvågning	14

9.5. Overvejelser i forbindelse med audit af understøttende it-systemer	14
10. Kommunikationssikkerhed	14
10.1. Styring af netværkssikkerhed	14
10.2. Styring af informationsoverførsel	15
11. Anskaffelse, udvikling og vedligeholdelse af it-systemer, applikationer m.m.	15
11.1. Sikkerhedskrav til it-systemer, applikationer	15
12. UnderEntreprenørforhold/forsyningskæden	16
12.1. Informationssikkerhed i underentreprenørforhold	16
12.2 Styring af underentreprenørydelser.....	17
13. Risikostyring.....	18
13.1. Risikovurderinger	18
13.2. Egenkontroller af Rammeaftalen	19
13.3. Deltagelse i kontrolaktiviteter og tilsyn/audits	19
14. Styring af Informationssikkerhedsbrud	20
14.1. Håndtering af informationssikkerhedshændelser.....	20
15. Informationssikkerhed i beredskabsstyring	23
15.1. Informationssikkerhedskontinuitet.....	23
16. Compliance med informationssikkerhed.....	24
16.1. Overensstemmelse med lov- og kontraktkrav	24
16.2. Ejerskab over Informationerne	24

Definitioner og referencer

Kontaktperson:	Med Kontaktperson menes den medarbejder, som af Entreprenøren er udpeget til at have det udførende ansvar for informationssikkerheden i relation til Rammeaftalen. Medarbejderen kan være udpeget som "Informationssikkerhedschef".
Informationer:	Med Informationer menes alle de informationer (herunder personoplysninger), data, fysiske dokumenter, materiale, tegninger m.v., der beskriver forhold inden for Forsvarsministeriets koncern.
Koncern:	Med Koncern refereres til Forsvarsministeriets koncern, herunder alle myndigheder.
Aktiv:	Med Aktiv menes alle assets, f.eks. it-system, applikation, netværk, underentreprenør m.v., som anvendes i Rammeaftalen.

1. Generelle krav til cyber- og informationssikkerhed

Nærværende kontraktbilag fastsætter Ejendomsstyrelsens krav til cyber- og informationssikkerhed i aftaleforholdet mellem Entreprenøren og Ejendomsstyrelsen for Rammeaftalen. Kontraktbilaget har til formål at beskytte de omfattede informationer under Entreprenørens behandling, lagring og transmission under opretholdelse af informationernes fortrolighed, integritet og tilgængelighed.

Da Rammeaftalen medfører behandling af fortrolige eller følsomme personoplysninger, er Entreprenøren desuden forpligtet til at tilslutte sig en databehandlersaftale med Ejendomsstyrelsen, jf. separat kontraktbilag. Databehandlersaftalen omhandler særskilte krav til beskyttelse af disse personoplysninger, som evt. underentreprenør også skal efterleve, bl.a. stilles krav om hurtig og sikker rapportering af persondatabrud forbundet med Rammeaftalen.

Som offentlig myndighed under Forsvarsministeriet er Ejendomsstyrelsen underlagt krav om at følge principperne i den internationale informationssikkerhedsstandard IEC/ISO 27001. Kravene i dette bilag er således dels baseret på denne standard dels på Forsvarsministeriets bestemmelsesgrundlag, herunder bestemmelser for den militære sikkerhedstjeneste, FKOBST 358-1, jf. www.fe.ddis.dk. Desuden skal kravene for håndtering af klassificerede informationer generelt efterleves, jf. Justitsministeriets sikkerhedscirkulære nr. 10338 af 17. december 2014 (Sikkerhedscirkulæret).

Ejendomsstyrelsen forbeholder sig retten til at pålægge Entreprenøren yderligere forpligtelser til cyber- og informationssikkerheden forbundet med Rammeaftalen, såfremt Ejendomsstyrelsen bliver pålagt at efterleve skærpede krav, f.eks. fra en overordnet myndighed, i forlængelse af et øget trussel- og risikobillede, lovgivningen, eller som følge af den generelle udvikling inden for informationssikkerhed, herunder også persondatabeskyttelse.

Generelt kan Entreprenøren med fordel opsøge vejledning om implementering af kravene i de internationale standarder inden for cyber- og informationssikkerhed, henholdsvis ISO/IEC 27002 og ISA/EC 62443 for så vidt angår operationel teknologi i automatiserings- og kontrolsystemer.

2. Informationssikkerhedspolitikker

2.1. Styringsgrundlag for informationssikkerhed

- 2.1.1. På grundlag af nærværende Rammeaftale samt tilhørende bilagsmateriale skal Entreprenøren udarbejde og vedligeholde de nødvendige interne informationssikkerhedspolitikker, proces- og procedurebeskrivelser til håndtering af Rammeaftalen. Disse skal udleveres til Ejendomsstyrelsen på anmodning.

3. Organisering af informationssikkerhed

3.1. Intern Organisering

- 3.1.1. Entreprenøren skal udarbejde og vedligeholde dokumentation for deres interne informationssikkerhedsorganisation for så vidt angår Rammeaftalen.

Entreprenøren skal over for Ejendomsstyrelsen udpege en Kontaktperson, som har det udførende ansvar for informationssikkerheden i Rammeaftalen, evt. med rollen som Informationssikkerhedschef.

Ved væsentlige ændringer i organiseringen ved Entreprenøren, skal Entreprenøren fremsende ny dokumentation med ændringerne uden yderligere varsel. Hvis der er tale om ny Kontaktperson, skal direkte telefonnummer og e-mailadresse være inkluderet.

3.2. Mobilt Udstyr

- 3.2.1. De af Koncernens Informationer, som er klassificerede, må alene lagres og behandles på det af Ejendomsstyrelsen udleverede mobile udstyr.

Entreprenøren skal til enhver tid følge de for transmission, behandling og lagring af Koncernens Informationer fastsatte retningslinjer, herunder understøttende instrukser til håndtering for Informationerne, klassificerede og ikke klassificerede.

- 3.2.2. På Entreprenørens eget mobile udstyr skal følgende minimumskrav håndhæves:

- *Full disk* kryptering
- Beskyttelse mod *malware*
- Adgangskode
- Fjernadgang (VPN mv.) må kun gives mod validering med brugernavn, adgangskode og to-faktor-godkendelse
- Entreprenøren skal føre en fortegnelse over fjernadgange, der som minimum inkluderer bruger, beskrivelse af behov for fjernadgang og tidsinterval for behovet.

4. Personalesikkerhed

4.1. Under ansættelsen

- 4.1.1. Entreprenøren skal pålægge de medarbejdere, der får eller kan få adgang til Koncernens Informationer, en fortrolighedsklausul med tavshedspligt omkring Rammeaftalen og Koncernens forhold, jf. bilag 5 (Militær sikkerhed), hvor gældende lovkrav fremgår.

For så vidt angår de af Entreprenørens medarbejdere, som sikkerhedsgodkendes, er de i forbindelse med den militære sikkerhedsgodkendelsesproces forpligtet til at tilslutte sig oplysningsskema med krav om tavshedspligt vedr. Rammeaftalen og Koncernens forhold i øvrigt, jf. bilag 5 (Militær sikkerhed).

Entreprenøren skal sikre, at alle medarbejdere, der opnår eller kan opnå adgang til klassificerede Informationer, er sikkerhedsgodkendt på rette niveau, og at sikkerhedsgodkendelsen opretholdes under hele perioden, hvor den enkelte medarbejder har adgang til Koncernens klassificerede Informationer eller udstyr.

Entreprenøren skal opretholde en opdateret fortegnelse over medarbejdere, der opnår eller kan opnå adgang til klassificerede Informationer med anførelse af personlig sikkerhedsgodkendelsesniveau. På anmodning skal Entreprenøren udlevere denne interne fortegnelse til Ejendomsstyrelsen.

- 4.1.2. Entreprenøren skal sikre, at medarbejdere der arbejder på Rammeaftalen, modtager instruks om hvordan Koncernens Informationer skal behandles, både klassificerede Informationer og ikke klassificerede Informationer.

Instruks til og træning af medarbejderne skal som minimum gennemføres årligt.

4.2. Ansættelsesforholdets ophør eller ændring

- 4.2.1. Entreprenøren skal gøre fratrædende medarbejdere opmærksomme på gældende fortrolighedsaftaler, herunder tavshedspligten, samt at disse forpligtelser ikke ophører ved ansættelsesophør, ændring i jobfunktion eller Rammeaftalens aftaleophør.

Entreprenøren skal sikre, at medarbejdernes adgang til Koncernens Informationer og udstyr med adgang hertil, slettes og/eller tilbageleveres i forbindelse med ansættelsesforløbets ophør, ændring i medarbejderens jobfunktion eller Rammeaftalens aftaleophør.

Entreprenøren skal sikre sig, at Koncernens Informationer på fratrædende medarbejders it-udstyr slettes.

Entreprenøren indestår for, at medarbejderne ikke i arbejdets medfør (tjenstligt) skal/må transmittere, behandle eller lagre Koncernens Informationer på medarbejderens private it-udstyr, herunder mobiltelefon. Entreprenøren er forpligtet til at gøre alle medarbejderne bekendte med sådan forbud om brug privat it-udstyr i forbindelse med Rammeaftalen.

5. Styring af aktiver

5.1. Ansvar for aktiver

- 5.1.1. Entreprenøren skal føre en fortegnelse over de aktiver, herunder it-systemer, applikationer, netværk (it-infrastruktur), der anvendes i relation til Rammeaftalens ikke klassificerede Informationer.

Minimumskrav til Entreprenørens aktivfortegnelse:

- Type af aktiv
- Beskrivelse af aktivet, herunder netværk
- Aktivets betydning for Rammeaftalen, herunder kritikalitet
- Aktivets ejer
- Kontaktperson til aktiv (superbruger eller administrator)
- Aktivets softwareinstallationer med oplysning om; entreprenør, versionsnumre, nuværende installationsstatus, ansvarlig for softwaren.

- 5.1.2. Tilsvarende skal Entreprenøren føre fortegnelse over det af Ejendomsstyrelsen udleverede it-udstyr til håndtering af Koncernens klassificerede Informationer.

Entreprenørens fortegnelsen over det af Ejendomsstyrelsen udleverede it-udstyr skal indeholde:

- Type af it-udstyr (FAP/FIA, usb, ekstern harddisk m.m.)
- Registreringsnummer
- Dato for modtagelse fra Ejendomsstyrelsen
- Navn på Entreprenørens bruger
- Formål med brug
- Dato for returnering til Ejendomsstyrelsen

- 5.1.3. Entreprenøren skal udarbejde en intern politik for accepteret brug, både af ikke klassificerede Informationer og aktiver og af klassificerede Informationer og it-udstyr omfattet af

Rammeaftalen i overensstemmelse med nærværende samt de til enhver tid fastsatte retningslinjer, herunder understøttende instrukser til håndteringen.

For så vidt angår Koncernens ikke klassificerede Informationer skal det understreges, at disse aldrig må deles eller lagres på sociale medier, cloud-løsninger, SaaS som f.eks. Dropbox, Google Drive eller lign., ud over det med Ejendomsstyrelsen aftalte.

Koncernens klassificerede Informationer må udelukkende transmitteres, behandles og lagres på Koncernens it-udstyr og netværk i Koncernens fastsatte retningslinjer, herunder understøttende instrukser til håndtering for klassificerede Informationer.

- 5.1.4. Entreprenøren indestår for at forpligte de medarbejdere, der får stillet Koncernens it-udstyr til rådighed og har adgang til Informationerne, til at tilbagelevere alt udleveret materiale, når den enkelte medarbejder ikke længere har et arbejdsbetinget behov for brugen/adgangen.
- 5.1.5. Entreprenøren skal opsætte intern procedure for at indsamle og videregive relevant viden, som den enkelte medarbejder har oparbejdet, inden denne skifter jobfunktion eller fratræder sin stilling hos Entreprenøren.

5.2. Mærkning af informationer

- 5.2.1. Entreprenøren skal beholde al mærkning og militær klassifikation af Koncernens Informationer og it-udstyr. Mærkningen og klassifikationen må ikke på et senere tidspunkt ændres eller nedklassificeres. Det er alene Ejendomsstyrelsen, som kan iværksætte ændring af klassifikation eller mærkning i relation til Rammeaftalen.

Entreprenøren må ikke påføre egne mærkninger på det til Rammeaftalen udleverede materiale fra og om Koncernen, ikke uden forudgående skriftlig godkendelse fra Ejendomsstyrelsen.

5.3. Mediehåndtering

- 5.3.1. Entreprenøren må ikke selv bortskaffe de af Ejendomsstyrelsen udleverede flytbare medier, f.eks. usb og eksterne harddiske. Koncernens it-udstyr, herunder flytbare lagermedier, skal altid tilbageleveres til Ejendomsstyrelsen.

Entreprenøren skal sikre, at indhold på egne flytbare medier, hvorpå Koncernens ikke klassificerede Informationer har været behandlet eller lagret, skal slettes på en uoprettelig måde. Metoden herfor skal forlods godkendes af Ejendomsstyrelsen, inden medierne må bortskaffes.

- 5.3.2. Lagermedier til opbevaring af militært klassificerede Informationer er tilsvarende klassificerede og skal udleveres af Ejendomsstyrelsen. Klassificerede lagermedier er krypterede.

Klassificeret udstyr skal altid være slukket under transport.

- 5.3.3. Ved forsendelse af lagermedier skal de være emballeret på en sådan måde, at det er umuligt at se hvad indholdet er.

6. Adgangsstyring

6.1. Forretningsmæssige krav til adgangsstyring

- 6.1.1. Entreprenøren udarbejder og vedligeholder et internt regelsæt for adgangsstyring i it-systemer m.v., hvor Koncernens Informationer skal behandles og lagres.

Regelsættet skal som minimum omhandle:

- Overensstemmelse mellem adgangsrettigheder og arbejdsmæssigt behov (*need-to-know* princip)
- Adgangsbegrænsning der sikrer, at klassificeret materiale eller udstyr alene kan tilgås af medarbejdere med rette personlige sikkerhedsgodkendelse
- Fastsættelse af regelmæssig gennemgang af adgangsrettigheder
- Løbende sletning af adgangsrettigheder, når de ikke længere er arbejdsbetingede
- Rollebeskrivelse for privilegerede adgangsrettigheder.

- 6.1.2. Entreprenøren skal sikre, at brugere/medarbejderne kun har adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte i relation til Rammeaftalen i overensstemmelse med regelsættet for adgangsstyring.

6.2. Tildeling og administration af brugeradgang

- 6.2.1. Entreprenøren skal have en intern proces for tildeling af almindelige brugerrettigheder.

Processen skal som minimum indeholde:

- Godkendelsesprocedure
- Rettighedstildeling gennem definerede roller
- Justering af tildelte brugerrettigheder ved ny jobfunktion eller stilling ved Entreprenøren.

- 6.2.2. Tilsvarende skal Entreprenøren have en intern proces for tildeling af privilegerede rettigheder (administratorrettigheder).

Processen skal som minimum indeholde:

- Godkendelsesprocedure for udpegning af administrator
- Entydigt bruger-id for bruger med privilegerede rettigheder
- Bruger med privilegerede rettigheder skal styre disse på en separat brugerkonto, hvor al adgang til respektive aktiv er identificerbar, dvs. medarbejdere med denne rolle også skal have brugerkonto med almindelige rettigheder
- Privilegerede rettigheder skal udelukkende tildeles ud fra et jobbetiget behov (*need-to-know* princip)
- Privilegerede rettigheder skal kunne tilskrives en specifik person.

- 6.2.3. Entreprenøren skal have intern procedure for brugeradministration.

Proceduren skal som minimum indeholde:

- Beskrivelse af krav til brugerregistrering og -afmelding, herunder øjeblikkelig spærring af brugere, der fratræder Entreprenørens virksomhed eller hvis jobfunktioner ændres til ikke længere at skulle arbejde med Rammeaftalen
- Krav om entydigt bruger-id
- Regelmæssig gennemgang af registrerede brugere for at identificere/spærre evt. brugere uden arbejdsbetinget behov (*need-to-know* princip), bl.a. ved ændringer i medarbejderes rolle, jobfunktion eller stilling og som minimum årligt og for privilegerede rettigheder som minimum halvårligt
- Enhver gennemgang skal være dokumenterbar
- Ændringer i autorisationer til privilegerede rettigheder skal logges
- Beskyttelse mod tildeling af nedlagt bruger-id til nye brugere.

6.2.4. Entreprenøren skal have proces for inddragelse af brugeradgange.

Processen skal som minimum indeholde:

- Inddragelse af brugerrettigheder, senest ved ophør af ansættelsesforhold
 - Om brugerrettighederne skal inddrages omgående eller ved opsigelsesvarslets ophør, afgøres ud fra kriterier som f.eks. hvem der har taget initiativ til ansættelsesophøret, medarbejderens tildelte ansvar, værdi/kritikalitet for de rettighedsberettigede aktiver
- Inddragelse/ tilpasning af brugerrettigheder ved ændringer i medarbejderens rolle, jobfunktion eller stilling
- Al inddragelse af brugerrettigheder skal logges.

6.2.5. Entreprenøren skal have intern proces for styring og tildeling af autentifikation som adgangskoder, chipkort m.m.

Processen skal som minimum indeholde:

- Krav om hemmeligholdelse af adgangskoder
- Krav om at midlertidig adgangskode skal ændres i forbindelse med første log-in
- Metode til at verificere behov, før adgangskode o.lign. udstedes eller ændres
- Krav om at producents standard adgangskode skal ændres efter installation, f.eks. af it-systemer eller software.

6.3. Brugernes ansvar

6.3.1. Entreprenøren skal tilsikre, at alle medarbejdere, herunder evt. underentreprenørers medarbejdere, følger Entreprenørens proces for brug af adgangskoder, chipkort eller tilsvarende i forbindelse med Rammeaftalen.

Processen skal som minimum fastsætte brugeransvar for:

- Fortrolig behandling af autentifikationsmetode (adgangskoder, krypteringsnøgler, chipkort eller lign., som ikke må videregives eller deles)
- Ingen registrering af autentifikationsmetoden, f.eks. på papir eller i en softwarefil, medmindre der er tale om en godkendt lagringsmetode som f.eks. password manager
- Ændring af autentifikationsmetoden ved enhver mistanke om kompromittering

- Brug af stærke adgangskoder, der ikke kan gættes
- Ændring af midlertidige adgangskoder ved første log-on
- Brug af sikker adgangskode ved automatisk log-on
- Ingen genanvendelse af samme adgangskoder, hverken anvendt i andre private eller erhvervsmæssige sammenhænge
- Aktivering af skærmlås, når medarbejder forlader arbejdsplads (også under arbejdstid).

6.4. Styring af system- og applikationsadgang

- 6.4.1. Entreprenøren skal have intern proces for begrænsning af adgang til it-systemer og applikationer, hvor Koncernens Informationer er tilgængelige.

Processen skal som minimum beskrive:

- Styring af den enkelte brugers adgang til it-systemer og applikationer
- Implementering af *least privilege*, hvor brugeren kun opnår adgang til et absolut minimum af it-systemer og applikationer ud fra et arbejdsbetinget behov (*need-to-know*)
- Begrænsning af den mængde af Informationer, der kan trækkes ud.

- 6.4.2. Entreprenøren skal have proces for sikker log-on.

Processen skal som minimum indeholde:

- Valg af passende autentifikationsmetode til verifikation af brugers identitet, f.eks. kryptografi eller *token*
- Kun et minimum af oplysninger om it-systemet eller applikationen for at undgå at en uautoriseret bruger opnår ikke-funktionsbetinget viden
- Ingen hjælpemeddelelser under log-on-proces
- Først validering af log-on, når alle oplysninger er registreret, for ikke at angive specifikt hvilke oplysninger, der måtte være korrekte eller forkerte
- Logning af fejlslagne og gennemførte forsøg på log-on med dato og tidspunkt
- Ingen visning af adgangskoder på skærmen under indtastning
- Ingen transmission af adgangskoder i klar tekst over et netværk
- Automatisk afslutning af inaktive sessioner på mobile enheder efter 3 timer
- Aktivering af pauseskærm med adgangskode efter 15 minutter.

- 6.4.3. Entreprenøren skal have proces for sikker brug af passwords.

Processen skal som minimum indeholde disse krav til brugerkonto med almindelige brugerrettigheder:

- Brug af personlig bruger-id og autentifikationsmetode/adgangskode for at sikre sporbarhed
- Valg og ændring af egne adgangskoder er op til den enkelte bruger
- Ændring af adgangskode ved første log-on
- Adgangskoder skal være komplekse og indeholde både store og små bogstaver, tal og tegn
- Adgangskoder må ikke kunne ses på skærmen under indtastning

- Lagring af filer med adgangskoder skal være adskilt fra applikationssystemdata
- Lagring og transmission af adgangskoder skal være krypteret.

6.4.4. Entreprenøren skal have proces for brug af systemprogrammer.

Processen skal som minimum beskrive:

- Adskillelse af systemprogrammer fra applikationssoftware
- Begrænsning i brugen af systemprogrammer til et minimum af betroede og autoriserede brugere (*least privilege*)
- Logning af brug af systemprogrammer
- Deaktivering og/eller fjernelse af alle unødvendige systemprogrammer
- Funktionsadskillelse.

7. Kryptografi

7.1. Kryptografiske kontroller

7.1.1. Entreprenøren udarbejder og vedligeholder dokumentation for anvendelsen af kryptografi i forbindelse med Rammeaftalen, der skal udleveres til Ejendomsstyrelsen efter anmodning herom.

Entreprenøren skal altid anvende stærk kryptering (pt. minimum TLS 1.2 og 256 bit), når kryptering anvendes.

8. Fysisk sikring og miljøsikring

8.1. Sikre områder

8.1.1. Entreprenøren skal opretholde en virksomhedssikkerhedsgodkendelse fra Forsvarets Efterretningstjeneste under hele aftalens løbetid.

Se nærmere om virksomhedsgodkendelse i bilag 5 (Militær sikkerhed).

8.1.2. Entreprenøren skal beskytte områder, der indeholder Koncernens Informationer med passende adgangskontroller, for at sikre kun autoriserede medarbejdere kan få adgang.

Se øvrige krav til fysisk sikkerhed i bilag 5 (Militær sikkerhed).

8.2. It-Udstyr

8.2.1. Entreprenøren skal sikre, at den fysiske placering af it-udstyr, der anvendes i Rammeaftalens opgaveløsning, beskyttes på en måde, hvor risici og trusler for f.eks. miljøtrusler og uautoriseret adgang reduceres.

8.2.2. Entreprenøren skal sikre, at it-udstyr i Rammeaftalen beskyttes mod strømsvigt og andre driftsforstyrrelser som følge af svigt af understøttende forsyning.

8.2.3. Entreprenøren skal sikre, at eget it-udstyr i Rammeaftalen vedligeholdes og opdateres korrekt for at sikre dets fortsatte tilgængelighed og integritet.

8.2.4. Entreprenøren skal sikre, at al it-udstyr med Koncernens Informationer uden for Entreprenørens domicil/lokation, f.eks. hjemmearbejdspladser, midlertidige arbejdspladser,

under rejser m.v. skal foretages under hensyntagen til de respektive risici forbundet hermed.

- 8.2.5. Entreprenøren indestår for, at ingen af Koncernens Informationer, hverken klassificerede, forretningskritiske eller ikke klassificerede Informationer, vil blive behandlet på medarbejderes private udstyr.

Tilsvarende indestår Entreprenøren for, at Koncernens klassificerede Informationer alene vil blive behandlet på Koncernens it-udstyr, udleveret af Ejendomsstyrelsen, og på Koncernens netværk i overensstemmelse med Koncernens understøttende instrukser til håndtering.

- 8.2.6. Entreprenøren skal sikre, at Koncernens Informationer er slettet/destrueret fra it-udstyr, herunder lagringsmedier, inden det bortskaffes. Sletning/destruktion skal foretages på en måde, hvor Koncernens Informationer ikke kan genfindes.
- 8.2.7. Materiale med de klassificerede Informationer skal returneres sammen med det Ejendomsstyrelsen udleverede it-udstyr. Entreprenøren skal til enhver tid følge Koncernens fastsatte retningslinjer, herunder understøttende instrukser for udlevering og aflevering af Koncernens Informationer og it-udstyr.

9. Driftssikkerhed

9.1. Driftsprocedurer og ansvarsområder

- 9.1.1. Entreprenøren skal styre organisationsændringer, ændrede forretningsprocesser, faciliteter og it-systemer, på en måde, som sikrer fortsat overholdelse af Ejendomsstyrelsens fastsatte informationssikkerhedsniveau og dermed –krav for Rammeaftalen.
- 9.1.2. Entreprenøren skal overvåge og tilpasse anvendelsen af ressourcer, og evt. fremskrive fremtidige kapacitetskrav, for til stadighed at kunne opretholde det for Rammeaftalen fastsatte informationssikkerhedsniveau.

9.2. Beskyttelse mod malware

- 9.2.1. Entreprenøren skal anvende passende anti-virus software i relation til Rammeaftalen, således Entreprenørens it-systemer er beskyttede mod malware.

Entreprenørens beskyttelse skal omfatte tiltag til detektering og forhindring af malware.

Disse tekniske foranstaltninger skal kombineres med passende instruks og brugerbevidsthed ved medarbejderne, så de er i stand til at identificere malware-forsøg.

9.3. Backup

- 9.3.1. Entreprenøren skal sikre, at der er en funktionel backup, som kan sikre genskabelse af Koncernens Informationer, andre nødvendige data eller software efter et nedbrud.

Entreprenøren skal foretage regelmæssige tests af backup-faciliteterne for at kunne validere deres effektivitet i nødsituationer.

9.4. Logning og overvågning

- 9.4.1. Entreprenøren skal sikre, at hændelseslogning af registrerede brugeraktivitet, afvigelser, fejl og informationssikkerhedshændelser vedrørende Rammeaftalen udføres, opbevares og gennemgås regelmæssigt.

Hændelsesloggen skal opbevares i mindst 13 måneder, medmindre der er indeholdt personoplysninger. I sådanne tilfælde skal personoplysningerne udtages og håndteres i overensstemmelse med gældende lovgivning samt **bilag 6 (Databehandleraftale)**.

- 9.4.2. Entreprenøren skal beskytte logningsfaciliteter og log-oplysninger om Rammeaftalen mod manipulation, overskrivning, sletning og uautoriseret adgang.

Entreprenøren skal desuden sikre at systemlogge beskyttes særligt, således at det opda-
ges, hvis loggen ændres.

- 9.4.3. De af Rammeaftalens aktiviteter, der udføres af systemadministratorer og systemoperatører, skal logges. Entreprenøren skal have en proces for beskyttelse af en sådan logning af systemadministrative og -operative aktiviteter.

Processen skal som minimum indeholde:

- Sikring af sporbarhed for privilegerede brugere, så det er muligt at identificere hvem, der har foretaget hvad
- Kontrolaktiviteter af, at systemadministratorer og -operatører ikke selv kan ændre logs fra de it-systemer, som de har de administrative brugerrettigheder
- Logs over systemadministrative og -operative aktiviteter skal gennemføres regelmæssigt
- Konkret vurdering af relevant opbevaringsperiode for logfiler for hvert enkelt it-system, dog 13 måneder som minimum
- Overvågning af systemadministratorer og -operatørers administratoraktiviteter skal foretages i et hændelsessystem, f.eks. SIEM, som systemadministratoren og/eller -operatøren ikke har kontrol over.

- 9.4.4. Entreprenøren skal sikre, at alle it-systemer i forhold til Rammeaftalen er synkroniserede til samme referencetidskilde. Entreprenørens valg af referencetidskilde samt implementeringen heraf skal være dokumenterbar.

9.5. Overvejelser i forbindelse med audit af understøttende it-systemer

- 9.5.1. Entreprenøren skal sikre, at krav om audit og kontrolaktiviteter, der indebærer verificering af drift af understøttende it-systemer for Rammeaftalen, planlægges og aftales forud, for at minimere uregelmæssigheder og afbrydelser i Ejendomsstyrelsens forretningsprocesser.

10. Kommunikationssikkerhed

10.1. Styring af netværkssikkerhed

- 10.1.1. Entreprenøren skal implementere kontroller for at sikre Koncernens Informationer i netværk og beskyttede tjenester mod uautoriseret adgang.

Ved implementeringen skal Entreprenøren overveje følgende styringstiltag:

- Etableringen af ansvar og procedurer for styring af netværksudstyr
- Passende logning og overvågning
- Autentificering af it-systemer på netværket
- Begrænsning af systemforbindelsen til netværket.

10.2. Styring af informationsoverførsel

- 10.2.1. Entreprenøren skal udarbejde interne procedurer, processer og opsætte kontroller for sikker og passende informationsoverførsel i de it-systemer, applikationer m.m., der anvendes i Rammeaftalen.

Entreprenøren skal sikre, at medarbejderne orienteres om ikke at have samtaler om Rammeaftalen på offentlige steder eller gennem offentlige trådløse netværk (hotel, café, lufthavn osv.) og trådløse netværk uden adgangskode.

- 10.2.2. Entreprenøren skal sikre, at digital overførsel eller deling af ikke klassificerede Informationer fra Rammeaftalen beskyttes på en passende og sikker måde.

Entreprenørens e-mail domæne skal beskyttes med DMARC-protokollen for at sikre, at:

- Meddelelser beskyttes mod uautoriseret adgang, ændring eller DDoS angreb
- Korrekt adressering og transmission af meddelelsen anvendes
- E-mail servicen er pålidelig og tilgængelig.

Entreprenørens overlevering af Rammeaftalens behandlede ikke klassificerede Informationer kan foretages til Rammeaftalens kontaktperson ved Ejendomsstyrelsen eller via sikkerpost på www.ejendomsstyrelsen.dk med kontaktpersonens navn og/eller stabsnavn ved Ejendomsstyrelsen anført.

- 10.2.3. For så vidt angår klassificerede Informationer fra Rammeaftalen må disse ikke overføres eller deles med tredjemand, heller ikke selv om tredjemand skulle være i besiddelse af rette sikkerhedsgodkendelse.

Enhver deling af klassificerede Informationer forudsætter separat forlods godkendelse af Ejendomsstyrelsen, og må udelukkende forekomme på Koncernens it-udstyr og netværk og i øvrigt i overensstemmelse med de til enhver tid gældende understøttende instrukser.

11. Anskaffelse, udvikling og vedligeholdelse af it-systemer, applikationer m.m.

11.1. Sikkerhedskrav til it-systemer, applikationer

- 11.1.1. Før brug af applikationstjenester over offentlige netværk, skal Entreprenøren foretage foranstaltninger til at beskytte Informationerne. I den forbindelse understreges, at det kun er ikke klassificerede Informationer fra Rammeaftalen, der må transmitteres gennem disse offentlige netværk med passende sikkerhedsforanstaltninger.

Til det formål skal Entreprenøren sikre dokumentation for:

- Godkendelsesprocesser for hvem der kan godkende, udstede og underskrive vigtige transaktionsdokumenter med Informationerne
- At enhver beslutning om opfyldelse af kravene herunder er truffet på oplyst grundlag med kvittering eller andet dokumenterbart bevis for afsendelse og modtagelse af relevante Informationer, samt kontraktuelle vilkårs uafviselighed, f.eks. i udbuds- og kontraktprocesser
- Anvendt beskyttelse af Informationerne
- Anvendte sikringstiltag i forhold til Informationernes fortrolighed og integritet i ordretransaktioner, betalingsoplysninger, leveringsadresser og kvittering for modtagelse
- Fastsat informationssikkerhedsniveau til opretholdelse af Informationernes fortrolighed og integritet, når de indgår i ordrer
- Forebyggende tiltag mod tab og kopiering af Informationerne
- Valgte forsikringsvilkår.

12. UnderEntreprenørforhold/forsyningskæden

12.1. Informationssikkerhed i underentreprenørforhold

12.1.1. I det omfang Entreprenøren har planlagt eller påtænker at overlade dele af Rammeaftalen til en eller flere underentreprenører, skal Entreprenøren forlods indhente Ejendomsstyrelsens godkendelse hertil.

Inden opstart skal Entreprenøren fremsende en fortegnelse over alle underentreprenørforhold, som Entreprenøren påtænker at anvende i Rammeaftalen, til Ejendomsstyrelsen.

Listen over underentreprenører skal indeholde oplysninger om:

- Virksomhedens navn
- CVR-nr.
- Adresse
- Kontaktperson
- Beskrivelse af delopgaven/behandlingen
- Tidsramme
- Dokumentation for sikkerhedsgodkendelse, både evt. virksomhedsgodkendelse og for de underentreprenørens medarbejdere, der skal arbejde med Rammeaftalen.

Entreprenøren er forpligtet til på et hvilket som helst tidspunkt at dokumentere en komplet, opdateret fortegnelse over forsyningskæden af underentreprenører i Rammeaftalen til Ejendomsstyrelsen.

12.1.2. Såfremt den del af Rammeaftalen, som en af Ejendomsstyrelsen godkendt underentreprenør skal opfylde, indebærer udveksling, behandling eller lagring af klassificerede Informationer, er Entreprenøren ansvarlig for, at den pågældende underentreprenør er sikkerhedsgodkendt ved Forsvarets Efterretningstjeneste, både personsikkerhedsgodkendelse af relevante medarbejdere og evt. virksomhedsgodkendelse når dette er påkrævet.

Den rette sikkerhedsgodkendelse, herunder personel, skal være tildelt til den respektive underentreprenør, inden Entreprenøren må inddrage underentreprenøren og dennes medarbejdere i opgaveløsningen for Rammeaftalen.

Entreprenøren indestår over for Ejendomsstyrelsen, for at der ikke kan opnås adgang til klassificerede Informationer, før rette sikkerhedsgodkendelse er indhentet. Se også bilag 5 (Militær sikkerhed), herunder procedure for sikkerhedsgodkendelse.

- 12.1.3. Entreprenøren skal sikre, at den respektive underentreprenør pålægges minimum de samme forpligtelser som Entreprenøren for den del af Rammeaftalen, som den enkelte underentreprenør skal løse.

Entreprenøren er ansvarlig for at udarbejde skriftlig aftale med enhver underentreprenør i Rammeaftalen (underentreprenøraftale).

Underentreprenøraftalen skal som minimum omfatte:

- Tilsvarende forpligtelser som Entreprenøren er pålagt af Ejendomsstyrelsen
- Præcis og detaljeret beskrivelse af hvilken delopgave underentreprenøren skal løse, herunder hvordan de omfattede Informationer må transmitteres, behandles og lagres.
- Beskrivelse og evt. klassifikation af de omfattede Informationer
- Lovkrav som er gældende i relation til delopgaven, f.eks. hvis behandling af Koncernens Informationer omfatter fortrolige eller følsomme personoplysninger, så er Entreprenøren forpligtet til at indgå en (under)databehandleraftale med underentreprenøren
- Krav om opdateret fortegnelse over de af underentreprenørens medarbejdere, der er udpegede og retmæssigt sikkerhedsgodkendte til at kunne tilgå og/eller behandle Koncernens Informationer
- Ret til auditering af underentreprenørens processer og kontroller i relation til Rammeaftalen, både for Entreprenøren og for Ejendomsstyrelsen.

I evt. grænsetilfælde eller ved tvivl skal underentreprenøren forpligtes til at anmode Entreprenøren om præcist at fastsætte, hvad underentreprenøren under ingen omstændigheder må foretage sig i relation til Rammeaftalen.

- 12.1.4. Entreprenøren indestår over for Ejendomsstyrelsen, for at informationssikkerhedsniveauet, og dermed alle informationskravene herunder, efterleves i alle underentreprenørforhold i hele forsyningskæden.

12.2 Styring af underentreprenørydelser

- 12.2.1. Aftalevilkårene i en evt. underentreprenøraftale må udelukkende fastsættes inden for rammerne af nærværende kontrakt med Ejendomsstyrelsen.
- 12.2.2. Det påhviler Entreprenøren at føre kontrol med underentreprenørs opfyldelse af informationssikkerhedskravene herunder. Udførte kontrolaktiviteter og tilsyn med underentreprenørydelserne skal Entreprenøren således kunne dokumentere over for Ejendomsstyrelsen. Det gælder for de forhold, områder og vilkår, som Ejendomsstyrelsen konkret måtte have stillet, eller under aftaleforholdet stiller, krav om.

Desuagtet der ikke foreligger specifik krav herom fra Ejendomsstyrelsen, er Entreprenøren forpligtet til over for evt. underentreprenører som minimum at:

- Overvåge og gennemgå service- og informationssikkerhedsniveauer for løbende at verificere underentreprenørens efterlevelse
- Afholde regelmæssige statusmøder med underentreprenøren, også med henblik på at kontrollere efterlevelse af informationssikkerhedskravene herunder
- Foretage audits i underentreprenørforhold og gennemgå uafhængige auditorrapporter, herunder revisorerklæringer
- Følge op på og risikohåndtere identificerede trusler, risici og afvigelser relateret til underentreprenørs delopgaver
- Rapportere om informationssikkerhedsbrud forbundet med Rammeaftalen, og i den forbindelse gennemgå understøttende retningslinjer, proces- og procedurebeskrivelser
- Gennemgå underentreprenørens auditspor og registreringer af informationssikkerhedshændelser, driftsproblemer, nedbrud, lokalisering af fejl og driftsforstyrrelser i relation til Rammeaftalen/delopgaven
- Vurdere informationssikkerhedsaspekter ved underentreprenørens evt. behov for under-underentreprenørforhold, som skal forudsætte Entreprenørens forlods accept og dermed også godkendelse af Ejendomsstyrelsen
- Sikre, at underentreprenøren dedikerer tilstrækkelige kapaciteter og ressourcer og fastsætter realistiske mål og beredskabsplaner til at sikre opretholdelsen af det aftalte service- og informationssikkerhedsniveau, også i en underentreprenørydelse/delopgave, under et alvorligt nedbrud eller en katastrofe.

- 12.2.3. Entreprenøren skal sikre, at evt. ændringer i Rammeaftalens underentreprenørydelser styres.

Entreprenøren skal forlods underrette Ejendomsstyrelsen om planlagte ændringer i underentreprenørforhold for derved give Ejendomsstyrelsen mulighed for at gøre indsigelse mod dem.

En underretning om ændring i Rammeaftalens underentreprenørforhold skal være Ejendomsstyrelsen i hænde i god tid, før ændringen er planlagt til at træde i kraft. Såfremt klassificerede Informationer er omfattet af ændringen, skal det være før Entreprenøren igangsætter sikkerhedsgodkendelsesprocedure for påtænkt ny underentreprenør. Såfremt Ejendomsstyrelsen har indsigelser til ændringen, skal Ejendomsstyrelsen give meddelelse herom til Entreprenøren hurtigst muligt efter modtagelse af underretningen.

Enhver ændring i underentreprenørforholdene for Rammeaftalen skal fremgå af Entreprenørens samlede fortegnelse over brug af underentreprenører m.fl., se ovenfor.

13. Risikostyring

13.1. Risikovurderinger

- 13.1.1. Entreprenøren er forpligtet til at rapportere om resultaterne fra egne risikovurderinger vedrørende Rammeaftalen til Ejendomsstyrelsen. Entreprenørens risikovurderinger skal

medtage inputs fra evt. underentreprenørydelser, og skal gennemføres i hele aftaleperioden.

Entreprenøren skal som minimum gennemføre risikovurderinger af Rammeaftalen:

- Inden opstart af Rammeaftalen
- Årligt i aftaleperioden
- Ved væsentlige sikkerhedshændelser
- Ved væsentlige ændringer, f.eks. organisatoriske eller ejerforhold hos Entreprenøren, eller ved overvejelse om ny underentreprenør (udskiftning eller yderligere)
- På baggrund af resultater fra informationssikkerhedstilsyn/audits hos Entreprenøren eller i Rammeaftalens underentreprenørforhold.

- 13.1.2. Derudover skal Entreprenøren på opfordring fra Ejendomsstyrelsen gennemføre konkrete risikovurderinger, der adresserer aktuelle trusler og sårbarheder i forhold til Rammeaftalen. I den forbindelse vurderes sandsynligheden for og konsekvenserne ved, at disse måtte udmønte sig i konkrete sikkerhedshændelser.

13.2. Egenkontroller af Rammeaftalen

- 13.2.1. Under Rammeaftalen skal Entreprenøren gennemføre egenkontroller af interne processer og procedurer for at sikre kontinuerlig overholdelse af det af Ejendomsstyrelsen fastsatte informationssikkerhedsniveau, og dermed samtlige informationssikkerhedskrav herunder.

På anmodning er Entreprenøren forpligtet til at fremsende dokumentation for gennemførte egenkontroller vedrørende Rammeaftalen til Ejendomsstyrelsen.

- 13.2.2. I den udstrækning at resultaterne fra de gennemførte egenkontroller viser behov for justeringer i relation til efterlevelse af Rammeaftalen, er Entreprenøren forpligtet til uden unødigt ophold at iværksætte forebyggende eller udbedrende tiltag for at optimere Rammeaftalen. Det omfatter også evt. tilpasninger i interne processer og procedurer vedrørende Rammeaftalen.

Entreprenøren skal registrere hvilke korrigerende handlinger og tidspunkt herfor, der skal imødekomme identificerede afvigelser og andre behov for tilpasninger.

Dokumentation for Entreprenørens handleplan over optimeringstiltag skal fremsende til Ejendomsstyrelsen på anmodning.

13.3. Deltagelse i kontrolaktiviteter og tilsyn/audits

- 13.3.1. Det påhviler Entreprenøren at deltage aktivt i Ejendomsstyrelsens kontrolaktiviteter relateret til Rammeaftalen, herunder evt. tilsyn, som Ejendomsstyrelsen måtte vurdere relevante.

- 13.3.2. Ejendomsstyrelsen er berettiget til at iværksætte kontrolaktiviteter med krav om, at Entreprenøren skal dokumentere efterlevelse af det fastsatte service- og informationssikkerhedsniveau herunder. Kontrolaktiviteterne kan foretages ved at:

- Overvåge og gennemgå Entreprenørens løbende serviceraporter

- Anmode om dokumentation og/eller bekræftelse på efterlevelse i forbindelse med parternes løbende statusmøder
- Gennemgå indrapporterede informationssikkerhedsbrud eller mistanke herom
- Gennemgå Entreprenørens hændelseslog over internt registrerede driftsproblemer, nedbrud, lokalisering af fejl og driftsforstyrrelser m.v. i relation til Rammeaftalen
- Gennemgå Entreprenørens håndtering af de registrerede hændelser og identificerede problemer
- Gennemgå Entreprenørens vurdering af identificerede informationssikkerhedsaspekter ved brug af den enkelte underentreprenør
- Gennemgå hvordan Entreprenøren planlægger at fastholde tilstrækkelig kapaciteter og ressourcer til at sikre opretholdelse af det aftalte service- og informationssikkerhedsniveau i tilfælde af et alvorligt nedbrud eller en katastrofe.

- 13.3.3. Et tilsyn ved Entreprenøren skal varsles med minimum 30 dage, medmindre Ejendomsstyrelsen vurderer et konkret og presserende behov, i hvilke tilfælde kortere frist kan forekomme. Formålet med det konkrete tilsyn skal fremgå af varslet.

I forbindelse med et tilsyn skal Entreprenøren udlevere den nødvendige dokumentation for efterlevelse af informationssikkerhedsniveauet, og dermed informationssikkerhedskravene herunder. Ligesom Entreprenøren skal stille alle nødvendige oplysninger til rådighed for Ejendomsstyrelsens tilsyn.

Entreprenøren er indforstået med, at Ejendomsstyrelsen kan engagere tredjemand til at gennemføre en uafhængig audit af Rammeaftalen, evt. revisorerklæring som ISAE 3402 eller ISAE 3000 af specifik område eller delopgave. I så fald afholdes alle udgifter til tredjemand af Ejendomsstyrelsen.

- 13.3.4. I god tid inden afholdelse skal Entreprenøren fremsende meddelelse om tredjemands tilsyn, hvor Rammeaftalen eller dele heraf måtte være inkluderet.

Ejendomsstyrelsen kan til enhver tid anmode om at få adgang til Entreprenørens auditspor efter tredjemands tilsynsrapport.

Det understreges, at Entreprenøren ikke må inkludere klassificerede Informationer eller personoplysninger i tredjemands tilsynsaktiviteter uden forlods at have indhentet Ejendomsstyrelsens accept.

14. Styring af Informationssikkerhedsbrud

14.1. Håndtering af informationssikkerhedshændelser

- 14.1.1. Entreprenøren skal sikre, at ledelsesansvaret for håndtering af informationssikkerhedshændelser i relation til Rammeaftalen er defineret.

Alle roller og ansvarsområder for håndteringen skal være udpeget og kommunikeret på baggrund af de respektive medarbejders kompetencer, dvs. de enkelte medarbejdere skal være certificerede eller på måde kvalificeret til at varetage opgaverne forbundet med håndteringen af en informationssikkerhedshændelse.

- 14.1.2. Entreprenøren skal sikre, at alle medarbejdere har mulighed for og pligt til at indrapportere observerede informationssikkerhedshændelser, herunder svagheder, trusler, sårbarheder eller mistanke herom.

Entreprenøren skal udarbejde og implementere en procedure for rapportering og hændelseshåndtering for indberettede informationssikkerhedshændelser eller mistanke herom, i relation til Rammeaftalen.

Den interne proces skal som minimum indeholde:

- Kontaktpunkt for medarbejdernes indberetning ved Entreprenøren
- Entreprenørens medarbejders pligt til at indberette informationssikkerhedshændelser eller mistanke herom i evt. underentreprenørforhold, formodentligt gennemført af den ved Entreprenøren udpegede kontaktperson til underentreprenøren
- Tekniske tiltag til overvågning og detektering
- Logning af styringsaktiviteter i forbindelse med informationssikkerhedshændelser, herunder beredskabsaktiviteter
- Indsamling af bevismateriale, herunder identifikation, kronologisk dokumentation for ejerskab, kontrol, overførsel, analyse og disposition over fysiske eller elektroniske beviser (*chain of custody*)
- Analyse og vurdering af den indberettede informationssikkerhedshændelse
- Fejlafhjælpning, kontrolleret reetablering efter nedbrud
- Intern kommunikation i relevant og sikkerhedsmæssigt forsvarligt omfang under hensyntagen til klassifikation og *need-to-know* princippet
- Tilbage melding til den medarbejder, som har indberettet informationssikkerhedshændelsen.

Processen skal indeholde en handlingsanvisende guide, der beskriver korrekt reaktion ved observation af en informationssikkerhedshændelse eller mistanke herom, inden og ved indberetningen, f.eks. straks notere detaljer om type af hændelse, overtrædelse eller brud, opståede fejl, meddelelser på skærmen, afkoble netværk til pc uden at lukke den ned.

Entreprenøren skal sikre, at opsætning af de tekniske foranstaltninger i processen varetages af teknisk kompetente medarbejdere. Ligeledes skal analyse og vurdering af hver enkelt indberetning foretages af medarbejdere med de rette kompetencer herfor, inden indberetningen registreres og håndteres som et egentligt informationssikkerhedsbrud.

En indberettet hændelse kan enkeltvist vurderes uden behov for yderligere håndtering, men såfremt den samme type hændelse viser et mønster, skal Entreprenøren opsamle de gentagne indberetninger og håndtere det som et informationssikkerhedsbrud.

Se også mulighed for rådgivning i forbindelse med bevisindsamling ved Forsvarets Efterretningstjeneste Cyber Situations Center nedenfor.

- 14.1.3. Entreprenøren indestår for, at alle vurderede og analyserede informationssikkerhedshændelser og –brud af betydning for Rammeaftalen og/eller Koncernen straks rapporteres telefonisk til den i Rammeaftalen oplyste kontaktperson hos Ejendomsstyrelsen, samt at

Entreprenøren uden unødigt forsinkelse følger op med en e-mail herom til kontaktpersonen.

Som minimum skal vidererapporteringen til Ejendomsstyrelsen omfatte beskrivelse af de for informationssikkerhedsbruddet konstaterede forhold om:

- Ineffektiv sårbarhedsstyring
- Brud på Informationernes integritet, fortrolighed eller tilgængelighed
- Udarbejdet teknisk analyse
- Udført håndtering af svagthed, der har forårsaget eller været medvirkende til informationssikkerhedsbruddet
- Menneskelige fejl
- Indsamlede kriminaltekniske beviser
- Afvigelser fra Entreprenørens interne processer og procedurer for Rammeaftalen
- Brud på den fysiske sikkerhed
- Ukontrollerede systemændringer
- Fejl i software eller hardware
- Brud på adgangskontrollerne.

Såfremt Ejendomsstyrelsens kontaktperson ikke kan træffes direkte telefonisk, skal rapportering ske via telefon til FES Servicecenter (72813300) og e-mail sendes til: FES-KTP-SERVICECENTER@mil.dk.

- 14.1.4. I det omfang Entreprenøren har behov for hjælp til håndteringen af det konstaterede informationssikkerhedsbrud, der relaterer Rammeaftalen, skal Entreprenøren aftale de nærmere vilkår med Ejendomsstyrelsens kontaktperson for Rammeaftalen.

Indsamling af beviser ved et konstateret informationssikkerhedsbrud skal ske i samråd med Ejendomsstyrelsen, som koordinerer med Forsvarets Efterretningstjeneste/Center for Cybersikkerheds Cyber hotline +45 33370037.

- 14.1.5. Efter en vellykket håndtering af informationssikkerhedsbruddet skal Entreprenøren formelt meddele Ejendomsstyrelsen, at håndteringen er afsluttet. Det skal fremgå, hvad der konkret er foretaget samt hvilke konsekvenser det har fået, herunder retsligt efterspil eller evt. medarbejdersanktioner.

Derudover skal Entreprenøren sikre, at den viden, der er opnået ved analyse og håndtering af informationssikkerhedsbruddet, anvendes forebyggende til at nedsætte sandsynligheden for eller virkningen ved evt. fremadrettede informationssikkerhedsbrud relateret til Rammeaftalen.

- 14.1.6. I den udstrækning Entreprenøren er forpligtet til at opretholde passende kontakt med andre instanser omkring håndtering af informationssikkerhedsbrud, skal Ejendomsstyrelsen forlods orienteres om hvad Entreprenøren påtænker at vidensdele i relation til Rammeaftalen. Dog undtaget såfremt der er tale om myndigheder inden for Koncernen, dvs. Forsvarsministeriets koncern.

15. Informationssikkerhed i beredskabsstyring

15.1. Informationssikkerhedskontinuitet

- 15.1.1. Entreprenøren skal planlægge forebyggende tiltag for at kunne opretholde informations-sikkerhedsniveauet for Rammeaftalen i en nødbereðskabs-, reetablerings eller krisehånd-teringssituation. Det skal fremgå hvordan tiltagene skal tilpasses i forhold til dem, der er implementeret ved normal drift, samt hvilke kompenserende tiltag, der ville skulle iværk-sættes som erstatning for de implementerede foranstaltninger, der ikke ville kunne opret-holdes i situationen.

Entreprenøren skal udarbejde formelle beredskabsplaner (ved nøds-, reetablerings- eller katastrofesituationer) under antagelse af, at informationssikkerhedsniveauet skal kunne opretholdes i såvel kritiske situationer som under normale driftsvilkår.

- 15.1.2. I Entreprenørens beredskabsplanlægning skal fremgå, hvordan Entreprenøren vil skabe informationssikkerhedskontinuitet, samt vilkår for hvornår og hvordan kriseberedskabet ved Entreprenøren skal indkaldes.

Planerne skal være kommunikeret og tilgængelige for alle medarbejdere med en rolle i be-redskabet for Rammeaftalen. Såvel ansvar som opgaver for den enkelte skal være define-rede og opdaterede, som minimum halvårligt. Tilsvarende er gældende for vedligehol-delse af liste med kontaktoplysninger for alle involverede roller.

Entreprenøren skal i beredskabsplanen ligeledes have fastlagt, hvordan Ejendomsstyrelsen holdes løbende orienteret samt inddrages i relevant omfang.

- 15.1.3. Entreprenøren skal udarbejde og implementere interne processer, procedurer og kontrol-ler for informationssikkerhedskontinuitet for Rammeaftalen i tilfælde af en kritisk situa-tion.

Det skal som minimum fremgå heraf at:

- En passende ledelsesstruktur i en beredskabssituation eller lign. er på plads
- Beredskabspersonalet er udpeget med det nødvendige ansvar, bemyndigelse og kompetence til at håndtere et sikkerhedsbrud og opretholde informationssikker-hedsniveauet for Rammeaftalen
- Der er udarbejdet skriftlige planer og procedurer, der beskriver, hvordan Entre-prenøren opretholder informationssikkerhedsniveauet for Rammeaftalen og sik-rer informationssikkerhedskontinuiteten
- Der er fastsat kontrolaktiviteter i processer, procedurer og understøttende syste-mer og værktøjer i beredskabssituationer
- Der er fastsat kompenserende foranstaltninger for de eksisterende informations-sikkerhedsforanstaltninger, som ikke kan opretholdes i en kritisk situation.

- 15.1.4. Entreprenørens beredskabsplaner, herunder procedurer og processer, der skal fastholde informationssikkerhedskontinuiteten i Rammeaftalen, skal afprøves med jævne mellem-rum og som minimum årligt.

Derudover skal de gennemgås ved:

- Øvelser og tests af reetablering af data, herunder Informationerne, i understøttende it-systemer (*data restore test*) og fuld reetableringstest (*disaster recovery test*)
- Større organisationsændringer ved Entreprenøren
- It-relaterede ændringer, der kan påvirke Rammeaftalen

Ejendomsstyrelsen skal orienteres om resultaterne fra beredskabstests og -øvelser, herunder identificerede risici samt Entreprenørens mitigerende (forebyggende eller udbedrende) tiltag fremadrettede.

- 15.1.5. Entreprenøren skal verificere, gennemgå og evaluere informationssikkerhedskontinuiteten for Rammeaftalen.

I evalueringen skal Entreprenøren gennemgå validiteten og effektiviteten af de foranstaltninger, der skal sikre informationssikkerhedskontinuiteten, herunder understøttende it-systemer, processer, procedurer, kontroller og kompenserende foranstaltninger, under en beredskabsstyring af Rammeaftalen.

16. Compliance med informationssikkerhed

16.1. Overensstemmelse med lov- og kontraktkrav

- 16.1.1. Det påhviler Entreprenøren at identificere og efterleve al relevant lovgivning gældende for Rammeaftalen.

Entreprenøren skal derudover være compliant med relevante myndigheds-, branche- og kontraktkrav i relation til Rammeaftalen under hensyntagen til nærværende informationssikkerhedskrav.

- 16.1.2. Entreprenøren skal overholde/efterleve alle immaterielle rettigheder til understøttende løsninger, der anvendes i forbindelse med Rammeaftalen. I den forbindelse indestår Entreprenøren for at fritage Ejendomsstyrelsen for ethvert ansvar, såfremt Entreprenøren måtte bryde immaterielle rettigheder under opgaveløsningen af Rammeaftalen.

Entreprenøren må alene anskaffe it-udstyr, herunder software, gennem kendte og ansete kilder. Bevis for ejendomsretten til licenser mv. skal opretholdes under hele Rammeaftalens løbetid.

Ejendomsstyrelsen er ansvarlig for immaterielle rettigheder til it-udstyr udleveret til Entreprenøren i forbindelse med opgaveløsninger, indeholdende klassificerede Informationer.

16.2. Ejerskab over Informationerne

- 16.2.1. Ejendomsstyrelsen har samtlige rettigheder til alle udleverede og behandlede versioner af Informationerne under nærværende aftale, dvs. enhver råderet, adkomst, ejendomsret, ophavsret og anden rettighed til Koncernens Informationer, der i forbindelse med Rammeaftalen behandles eller lagres ved Entreprenøren. Det gælder også for de Informationer der i forbindelse med Rammeaftalen er behandlet eller lagret i Entreprenørens it-systemer eller it-infrastruktur, herunder metadata, logfiler, revisionsspor med Informationerne m.v.

I det omfang Ejendomsstyrelsen ikke selv kan foretage dataudtræk af Informationerne ved Entreprenøren, kan Ejendomsstyrelsen til enhver tid vederlagsfrit begære at få udleveret en kopi af alle eller dele af Koncernens Informationer på et relevant it-læsbart lagermedie (standard format uden transformeringer og risiko for datatab).

Udleveringen af dataudtrækket med Informationerne skal finde sted inden for en af Ejendomsstyrelsen fastsat frist, der står i rimeligt forhold til omfang af de Informationer, som ønskes udleveret.

Entreprenøren må ikke på noget tidspunkt eller på nogen måde tilbageholde Koncernens Informationer, som er i Entreprenørens besiddelse. Det gælder uanset om der mellem parterne måtte være opstået en tvist eller anden uoverensstemmelse, eller Ejendomsstyrelsen i øvrigt måtte have misligholdt sine forpligtelser herunder.

- 16.2.2. Desuagtet årsag til aftaleophøret skal Entreprenøren uden yderligere vederlag og på god og forsvarlig vis medvirke i overgangen til en ny løsning for Rammeaftalen. Enten ved at udlevere alt materiale relateret til Rammeaftalen, herunder it-udstyr og alle versioner af Informationerne, til Ejendomsstyrelsen eller en af Ejendomsstyrelsen udpeget tredje-
mand. Entreprenøren forpligter sig desuden til at bistå med opbygget viden med henblik på at kunne gennemføre overdragelsen uden unødige komplikationer.

Ved endeligt aftaleophør må Entreprenøren ikke være i besiddelse af Koncernens materiale, herunder it-udstyr, Informationer eller kopier heraf, helt eller delvist.

Tidspunkt for Entreprenørens returnering eller sletning aftales nærmere mellem parterne. Ved tvivl om omstændighederne herfor skal Entreprenøren rette henvendelse til Ejendomsstyrelsens kontaktperson i god tid inden aftaleophør med henblik på at aftale de nærmere vilkår for returnering eller sletning.