FORSVARSMINISTERIET
EJENDOMSSTYRELSEN

AFTALEBILAG 2.2

SIKKERHEDSKRAV – ADGANG TIL FORTROLIGE INFORMATIONER (*GRØN*)

Dato: 30. april 2024
KESDH sagsnummer: 2023/011768

Grønt bilag - Sikkerhedskrav – Adgang til fortrolige informationer

Nærværende bilag fastsætter militære sikkerhedskrav og informationssikkerhedskrav til leverandører som Forsvarsministeriets Ejendomsstyrelse (herefter Ejendomsstyrelsen) indgår kontrakter med.

Ejendomsstyrelsen er underlagt ISO 27001 (krav til informationssikkerhed) til behandling af oplysninger og data, og krav til militær sikkerhed jf. Forsvars-kommandobestemmelse 358-1 (FKOBST 358-1).

Derudover kan data være klassificeret, jf. Justitsministeriets sikkerhedscirkulære nr. 10338 af 17. december 2014 (sikkerhedscirkulæret), som stiller særlige krav til behandling.

Krav i bilaget:
Alle krav i bilaget er mindstekrav i forhold til den konkrete leverance.

Definitioner:
Ejendomsstyrelsen: Kunden/Forsvarsministeriets Ejendomsstyrelse.

Leverancen: Ydelsen som Ejendomsstyrelsen køber hos Rådgiveren.

Kontaktpersonen: Med Kontaktpersonen eller Kontaktperson menes der en fysisk person udpeget af Rådgiveren med ansvar for informationssikkerheden i relation til Leverancen.

Sikkerhedschef: Rådgiverens udpegede medarbejder med ansvaret for den militære sikkerhed.

INDHOLDSFORTEGNELSE

1. NEED TO KNOW

Forsvaret arbejder efter "need to know" princippet, hvilket betyder, at adgang til klassificeret information skal være påkrævet af hensyn til opgaveløsningen. Det gælder alle informationer og data fra Ejendomsstyrelsen. Stilling eller titel er ikke afgørende for adgangen til information. Der skal være overensstemmelse mellem adgang til informationer og det arbejdsmæssige behov.

2. SIKKERHEDSPOLITIKKER

Rådgiveren skal udarbejde og vedligeholde en informationssikkerhedspolitik. Formålet med politikken er at beskrive Rådgiverens rammer for arbejdet med informationssikkerhed. Politikken skal beskrive ledelsens valgte niveau for informationssikkerhed.
På sikkerdigital.dk kan Rådgiveren finde vejledning til udarbejdelse af politikken.

2.1 SIKKERHEDSINSTRUKS

Rådgiveren skal have en sikkerhedsinstruks vedr. militær sikkerhed, så Rådgiverens medarbejdere er bevidste om sikkerheden ved håndtering af klassificerede informationer. Sikkerhed handler bl.a. om at beskytte Forsvaret, herunder personel, materiel og etablissementer. Rådgiverne skal rette sig efter "Bestemmelse for den militære sikkerhedstjeneste" (FKOBST 358-1). Bestemmelsen er tilgængelig på Forsvarets Efterretningstjenestes hjemmeside[1]. Rådgiveren skal kende de sikkerhedsmæssige forpligtigelser.

3. ORGANISERING AF SIKKERHED

Rådgiveren skal udarbejde og vedligeholde dokumentation for deres interne organisation i forhold til informationssikkerhed og militærsikkerhed.

3.1 MÆRKNING AF INFORMATIONER

Informationer fra Ejendomsstyrelsen har en mærkning, som afgør, hvem der må få kendskab til informationerne, og hvilken grad Rådgiverens medarbejdere skal være sikkerhedsgodkendt til. Klassifikationsgraden som medarbejderne skal godkendes til, varierer afhængigt af arbejdets art og den fysiske lokation.

Klassifikationsgraderne er:
- UKLASSIFICERET
- TIL TJENESTEBRUG
- FORTROLIGT
- HEMMELIGT

Det er Ejendomsstyrelsen, der fastsætter klassifikationsgraden. Rådgiveren skal beholde Ejendomsstyrelsens mærkning og militær klassifikation af information og må ikke på et senere tidspunkt ændre eller nedklassificere eksisterende mærkninger.

Rådgiveren må ikke påføre egne mærkninger af information og udstyr uden forudgående skriftlig godkendelse fra Ejendomsstyrelsen

3.2 SIKKERHEDSGODKENDELSE

Rådgiverens medarbejdere, der skal have adgang til klassificeret information, skal sikkerhedsgodkendes. Medarbejderen skal være sikkerhedsgodkendt til det niveau, som informationen er klassificeret til.

Rådgiveren skal udarbejde og vedligeholde en liste med information om:
- Medarbejdere, der modtager eller kan få adgang til klassificerede informationer.

[1] Link til 358-1

- Sikkerhedsgodkendelsesniveau for de enkelte medarbejdere.
- Rådgiveren skal sikre at medarbejderne opretholder sikkerhedsgodkendelsen under hele perioden, hvor de har adgang til information fra Ejendomsstyrelsen.

Rådgiveren skal sikre at medarbejdere, der arbejder på leverancen til Ejendomsstyrelsen, modtager information om regelsæt for fysisk adgang til Forsvarsministeriets etablissementer, samt hvordan informationer og udstyr skal håndteres.

Informationen til Rådgiverens medarbejdere skal som minimum gentages årligt ved længerevarende opgaver.

3.3 VIRKSOMHEDSGODKENDELSE

Virksomheden/Rådgiveren skal sikkerhedsgodkendes, hvis Rådgiveren opbevarer klassificerede informationer, eller hvis et større antal medarbejdere[2] fra samme Rådgiver skal udføre arbejde for Ejendomsstyrelsen.

I forbindelse med virksomhedsgodkendelse, skal Rådgiveren oprette sin egen sikkerhedsorganisation. Virksomheden indstiller herefter egne medarbejdere og underleverandørers medarbejdere til sikkerhedsgodkendelse. Retningslinjerne findes i FKOBST 358-1, kap. 8.
Rådgiveren skal opretholde en virksomhedssikkerhedsgodkendelse fra Forsvarets Efterretningstjeneste under hele aftalens løbetid.

3.4 ANSVARLIG KONTAKTPERSON OG SIKKERHEDSCHEF

Rådgiveren skal udpege en **kontaktperson** til Ejendomsstyrelsen, der er ansvarlig for informationssikkerheden i den specifikke leverance.

Rådgivere der udfører klassificeret arbejde, skal ydermere udpege en **sikkerhedschef**. Sikkerhedschefen har ansvaret for udøvelse af den militære sikkerhed, herunder efterlevelse af sikkerhedsinstruksen, og for at Rådgiverens medarbejdere sikkerhedsgodkendes og afmeldes, når der ikke længere er brug for sikkerhedsgodkendelsen. Sikkerhedschefen skal have direkte reference til virksomhedens chef. Sikkerhedschefen kan tage kontakt til Ejendomsstyrelsens sikkerhedsofficer eller virksomhedssikkerhedssektionen i Forsvaret Efterretningstjeneste ved spørgsmål om militær sikkerhed.

Sikkerhedschefen og kontaktpersonen kan godt være den samme person.

4. UDSTYR

Udstyr og mobilenheder kan deles op i 3 grupper: Udstyr udleveret af Ejendomsstyrelsen, Rådgiverens eget udstyr og medarbejdernes private udstyr.

Rådgiveren skal sikre at udstyr placeres forsvarligt og beskyttes så muligheden for uautoriseret adgang minimeres.

Alle informationer fra Ejendomsstyrelsen skal slettes ved kontraktophør medmindre andet er aftalt eller Rådgiveren i henhold til anden lovgivning er forpligtet til at opbevare informationerne. Sletning skal ske ved hjælp af metoder, således at den oprindelige information ikke kan genfindes.

[2] Et større antal: Hvis der er tale om flere end 15 medarbejdere fra samme leverandør, er der grundlag for at sikkerhedsgodkende virksomheden.

4.1 UDSTYR UDLEVERET AF EJENDOMSSTYRELSEN

Klassificeret information TIL TJENESTEBRUG må kun håndteres på det udleverede udstyr fra Ejendomsstyrelsen, medmindre andet er aftalt.

Medier, der benyttes til opbevaring af militært klassificerede informationer, udleveres af Ejendomsstyrelsen, og skal altid være krypteret samt være slukket under transport.

Rådgiveren må ikke selv bortskaffe Ejendomsstyrelsens udstyr. Rådgiveren skal forpligte medarbejdere til at tilbagelevere udleveret udstyr fra Ejendomsstyrelsen, når der ikke længere er et arbejdsbetinget behov for brugen, eller senest ved kontraktophør eller fratrædelse.

Ved forsendelse skal medier emballeres på en sådan måde, at det er umuligt at se, hvad indholdet er.

Opstår der i forbindelse med udførelse af en opgave for Ejendomsstyrelsen behov for, at Rådgiveren skal kommunikere med klassificerede informationer, kan der udleveres en PC som fjernarbejdsplads. Udlevering og håndtering af Pc'en skal følge Ejendomsstyrelsens retningslinjer.

4.2 RÅDGIVERENS EGET UDSTYR

Klassificeret information Til TJENESTEBRUG må kun håndteres efter aftale med Ejendomsstyrelsen på Rådgiverens udstyr.

Rådgiveren skal sikre at udstyr, som anvendes til behandling eller opbevaring af Ejendomsstyrelsens informationer uden for Rådgiverens organisation, herunder hjemmearbejdspladser, midlertidige arbejdspladser, under rejser med mere, skal ske under hensyntagen til de forskellige risici, som dette måtte medføre.

Rådgiveren skal føre et register over fjernadgange, herunder brugere, beskrivelse af behov for fjernadgang og tidsinterval for behovet. Rådgiveren skal udarbejde og vedligeholde procedurer for anvendelsen af flytbare medier og mobilt udstyr (herunder eksempelvis USB Flash Drives og eksterne harddiske).

Rådgiveren skal sikre, at Ejendomsstyrelsens information er slettet fra udstyr inden udstyret bortskaffes.

4.3 PRIVAT UDSTYR

Rådgiveren skal udarbejde en politik for brug af information og aktiver i relation til leverancen.
Rådgiveren skal sikre, at Ejendomsstyrelsens informationer ikke overføres til eller tilgås fra medarbejderes private udstyr.
Rådgiveren er ansvarlig for, at medarbejderne ved, at det ikke er tilladt at anvende eller lagre informationer fra Ejendomsstyrelsen på sociale medier, cloud-løsninger, SaaS, f.eks. Dropbox, Google Drive eller tilsvarende.

4.4 DOKUMENTHÅNDTERING

Opbevarer Rådgiveren dokumenter klassificeret TIL TJENESTEBRUG skal disse opbevares bag dobbelt lås eksempelvis i et låst skab i et aflåst lokale.

Dokumenter klassificeret TIL TJENESTEBRUG kan sendes som alm. post og på FIIN (Forsvarets interne netværk), aldrig på internettet.

UKLASSIFICERET information kan håndteres på internettet.

5. STYRING AF AKTIVER

Rådgiveren skal føre fortegnelse over aktiver, herunder IT-systemer og IT-infrastruktur, der anvendes i relation til leverancen.

Krav til fortegnelsen:
- Navn
- Beskrivelse
- Betydning
- Ejerskab
- Kontaktperson
- Klassifikation

6. ADGANGSSTYRING

6.1 POLITIK

Udarbejde en politik som indeholder information om:
- Adgangsrettigheder og arbejdsmæssigt behov (need-to-know princip).
- Adgangsbegrænsning og regelmæssig gennemgang af adgangsrettigheder.
- Sletning af adgangsrettigheder.
- Beskrivelse af roller med privilegeret adgang.

6.2 BRUGERADGANGE

Procedure og krav til brugeradministration, privilegerede rettigheder og tildeling af rettigheder:
- Beskrivelse af godkendelse, brugerregistrering og afmelding.
- Entydigt bruger-id.
- Kontrol af adgange.
- Beskyttelse mod tildeling af nedlagt bruger-id til nye brugere.
- Tildeling af rettigheder gennem roller.
- Brugere med privilegerede rettigheder skal kunne identificeres for hvert aktiv.
- Brugere med behov for privilegerede rettigheder skal have en separat brugerkonto til dette formål.
- Rådgiveren skal gennemgå brugerrettigheder minimum hvert år, og på privilegerede adgangsrettigheder hver 6. måned.
- Ændringer i autorisationer til privilegerede rettigheder skal logges og gennemgås periodisk.
- Ved ændringer i rolle eller stilling, skal det afgøres om rettigheder skal tilpasses eller slettes.
- Hvis en fratrædende medarbejder har adgang til brugerkonti, der stadig vil være aktive, skal adgangskoder hertil ændres senest ved ansættelsesophør.

6.3 MEDARBEJDERNES ANSVAR

Rådgiveren skal tilsikre, at medarbejdere og underleverandører følger Rådgiverens praksis for brugen af adgangskoder, chipkort eller tilsvarende i forbindelse med leverancen:

- Rådgiverens medarbejdere skal behandle adgangskoder og anden autentifikationsinformation fortroligt.
- Autentifikationsinformation må ikke registreres på f.eks. papir eller i en softwarefil, medmindre det er en godkendt lagringsmetode (f.eks. password vault).
- Autentifikationsinformation skal ændres ved enhver mistanke om kompromittering.
- Sikre adgangskoder, når disse anvendes som autentifikationsinformation i automatiske log-on procedurer og lagres.
- Aldrig anvende samme adgangskoder til beskyttelse af Ejendomsstyrelsens information, der er anvendt i andre private eller erhvervsmæssige sammenhænge.
- Pauseskærm med adgangskode skal aktiveres på udstyr.
- Rådgiveren skal sikre, at medarbejdere låser skærmen hver gang de forlader udstyret.

6.4 SIKRE LOGON PROCEDURER

- Der skal vælges passende autentifikationsmetode til verifikation af brugeres påståede identitet, f.eks. kryptografi eller tokens.
- Log-on proceduren skal afsløre et minimum af information om systemet eller applikationen for ikke at give en uautoriseret bruger mere viden.
- Ikke give hjælpemeddelelser under log-on-proces.
- Først validere log-on-oplysningerne, når alle data er registreret og ikke angive hvilken del af dataene, der er korrekt eller forkert.
- Logge fejlslagne og gennemførte forsøg på log-on, inkl. dato og tid.
- Ikke vise adgangskoder på skærmen under indtastning.
- Ikke transmittere adgangskoder i klar tekst over et netværk.
- Afslutte inaktive sessioner på mobile enheder efter 3 timer.

6.5 ADGANGSKODER

- Adgangskoder skal holdes hemmelige.
- Rådgiver skal sikre midlertidig og individuelle adgangskode ved første log-in, der skal ændres ved første anvendelse.
- Procedure for verificering af identitet før en adgangskode kan udstedes eller ændres.
- Standard-adgangskoder fra leverandører skal ændres efter installation for systemer eller software.
- Anvend flerfaktor-autentifikation.
- Anvend passwordmanager til at gemme og generere passwords.
- Genbrug aldrig adgangskoder.
- Anvend stærke adgangskoder – god længde (15 tegn) og lavere kompleksitet.
- Anvend tvunget skift af koder med fast interval.

Se vejledning til *Passwordsikkerhed* fra Center for Cybersikkerhed for yderligere information om passwords.

7. LEVERANDØRFORHOLD

Rådgiveren skal sikre, at underleverandører er pålagt relevante forpligtelser, som Rådgiveren er pålagt af Ejendomsstyrelsen, så sikkerhedsniveauet ikke udvandes.
Rådgiveren skal udlevere en liste over underleverandører til Ejendomsstyrelsen.

Underleverandørlisten skal indeholde oplysning om:

- Virksomhedens navn
- CVR-nr.
- Adresse
- Kontaktperson
- Hvad virksomheden skal udføre for Rådgiveren
- Tidsrammen
- Dokumentation for at virksomheden og medarbejdere er sikkerhedsgodkendt på rette niveau.

Rådgiveren har ansvaret for at medarbejdere og underleverandører er sikkerhedsgodkendt til rette niveau, hvis der opbevares klassificeret information hos underleverandøren.

Rådgiveren er forpligtet til at informere Ejendomsstyrelsen om skift af underleverandører.

Skift af underleverandør skal ske med et varsel på 3 måneder, således det kan nås at sikkerhedsgodkende underleverandørers medarbejdere, medmindre andet aftales med Ejendomsstyrelsen.

8. SIKKERHEDSBRUD

8.1 BRUD ELLER MISTANKE OM SIKKERHEDSBRUD

Rådgiveren herunder medarbejdere og eventuelle underleverandør er forpligtede til at rapportere om brud eller mistanke om brud på militærsikkerhed, der konstateres under arbejdets udførelse. Rapporteringen foretages til Ejendomsstyrelsens sikkerhedsofficer. Forekommer der situationer, hvor den militære sikkerhed på Etablissementer berøres, og som skal løses med det samme, skal sikkerhedschefen kontaktes. Eksempelvis hvis en leverandør ude på en kaserne, ikke kan låse en dør.

Sikkerhedsbrud og hændelser vedr. informationssikkerhed skal rapporteres telefonisk uden unødig forsinkelse til den oplyste kontaktperson hos Ejendomsstyrelsen. Hvis kontaktpersonen ikke kan træffes, skal rapportering ske via telefon til Ejendomsstyrelsens Servicecenter (72813300) og via e-mail til: FES-KTP-SERVICECENTER@mil.dk.

8.2 HÅNDTERING AF SIKKERHEDSBRUD

Rådgiveren skal sikre, at ansvaret for håndtering af informationssikkerhedsbrud for den konkrete leverance er fastlagt.
Proceduren skal sikre at Rådgiverens medarbejdere kan håndtere sikkerhedsbrud, samt at Rådgiveren implementerer et kontaktpunkt for opdagelse og rapportering, og der etableres en passende kontakt med Ejendomsstyrelsen.

Ved informationssikkerhedshændelser (f.eks. DDos angreb, phishing, hacking) skal Rådgiveren:

- Indsamle beviser hurtigst muligt efter hændelsen.
- Afhjælpe fejl efter behov.
- Sikre at alle involverede beredskabsaktiviteter logges korrekt for senere analyse.
- Underrette Ejendomsstyrelsen.
- Håndtere informationssikkerhedssvagheder som har forårsaget eller været medvirkende til bruddet.
- Logge og registrere hændelse.

Rådgiveren skal sikre, at den viden, der opnås ved at analysere og håndtere sikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud. Informationer, der er indsamlet i forbindelse med sikkerhedsbrud, skal anvendes til identifikation af gentagne brud og brud med store konsekvenser.

9. BEREDSKAB

Krav til Rådgiverens beredskab. Rådgiveren skal:

- Klarlægge om informationssikkerhedskontinuiteten (Processer og procedure til sikring af uafbrudt efterlevelse af krav til informationssikkerhed) skal være forankret i nød-, beredskabs- og reetableringsstyringen eller i krisehåndteringen.
- Fastlægge sikkerhedskrav ved nød-, beredskabs- og reetableringsplanlægningen og krisehåndteringen.
- Udarbejde formelle nød-, beredskabs- og reetableringsplaner eller katastrofeplaner, hvor det antages at informationssikkerhedskravene er de samme i kritiske situationer som under normale driftsforhold.
- Udarbejde og implementere processer, procedurer og kontroller for informationssikkerhedskontinuitet i en kritisk situation.
- Verificere, gennemgå og evaluere informationssikkerhedskontinuiteten.
- Gennemgå validiteten og effektiviteten af foranstaltningerne i relation til informationssikkerhedskontinuiteten, informationssystemer, informationssikkerhedsprocesser, procedurer og kontroller eller processer og løsninger vedrørende nød-, beredskabs- og reetableringsstyring og krisehåndtering.

10. COMPLIANCE

Rådgiveren skal sikre at være i compliance med alle relevante lov-, myndigheds- og kontraktkrav, der er relevante for leverancen.

Rådgiveren skal identificere lovgivning, som gælder for deres organisation i forhold til leverancen for at kunne overholde denne.

Rådgiveren må alene anskaffe software gennem kendte og ansete kilder og skal opretholde bevis for ejendomsretten til licenser mv.

11. TILSYN OG INTERN KONTROL

Rådgiveren skal i relation til leverancen sikre, at Rådgiverens metode til styring af informationssikkerhed og implementeringen heraf gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.

Hvis Rådgiveren har indhentet en revisorerklæring (fx ISAE 3402 eller ISAE 3000), der er relevant i forhold til leverancen, skal Ejendomsstyrelsen underrettes herom, og på forlangende skal denne erklæring forelægges Ejendomsstyrelsen.

Rådgiveren skal i relation til leverancen sikre, at Rådgiverens ledelse regelmæssigt undersøger, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav. Rådgiveren skal på opfordring fra Ejendomsstyrelsen, udarbejde en risikovurdering, der identificerer aktuelle trusler og sårbarheder i forhold til Leverancen, samt vurderer sandsynligheden for – og konsekvensen hvis, disse trusler eller sårbarheder udmønter sig i konkrete sikkerhedshændelser.

Rådgiveren skal aktivt deltage i et eventuelt tilsyn, hvis Ejendomsstyrelsen finder anledning hertil.

Yderligere bemærkninger om Ejendomsstyrelsens tilsyn:

- Tilsyn kan både handle om efterlevelse af sikkerhedskravene såvel som øvrige kontraktuelle forhold i almindelighed.
- Ejendomsstyrelsen har ret til at føre tilsyn minimum årligt, eller ved væsentlige hændelser hos Rådgiveren.
- Rådgiveren varsles minimum 14 dage før et tilsyn.
- Rådgiveren forpligter sig til i nødvendigt omfang at deltage i, og stille nødvendige ressourcer og materialer/dokumentation til rådighed ved tilsyn, herunder at give fysisk adgang til Rådgiverens lokationer/faciliteter.
- Rådgiverens deltagelse i tilsyn skal foregå vederlagsfrit.
- Eventuelle relevante revisionserklæringer eller certificeringer Rådgiveren måtte have, kan ikke erstatte et fysisk tilsyn, såfremt Ejendomsstyrelsen vurderer der er behov herfor.

Rådgiveren skal føre tilsyn med underleverandører vedrørende de krav Ejendomsstyrelsen konkret har stillet i forhold til den konkrete aftale/leverance.