DANSKE Patruljeskibe

Version: 2023-10-02

VEJLEDNING OM ANSØGNINGSPROCES FOR MILITÆR SIKKERHEDSGODKENDELSE

1 FORMÅL

Danske Patruljeskibe (DPS) har indgået kontrakt med Forsvarsministeriet Materiel- og Indkøbsstyrelse (FMI) om nye patruljeskibe til Søværnet. Patruljeskibene er en del af Søværnets kampenheder, og Forsvaret har påpeget vigtigheden af, at ingen uvedkommende får adgang til klassificerede eller sensitive informationer om skibenes kapacitet, indretning eller udstyr.

Dette stiller særlige krav til DPS og vores kommende partnere og leverandører.

Denne vejledning tjener til formål, at danske virksomheder kan forberede sig på de sikkerhedskrav, projektet stiller, herunder at initiere ansøgning om sikkerhedsgodkendelse for virksomhed og for relevante medarbejdere. Ansøgnings- og godkendelsesprocessen for sikkerhedsgodkendelse kan vare op til 8 måneder.

2 ER VIRKSOMHEDEN ALLEREDE GODKENDT AF FE

Mange danske virksomheder har tidligere leveret ydelser eller udstyr til Forsvaret og har måske derfor allerede en gældende virksomhedsgodkendelse. I dette tilfælde anbefales følgende:

1. Kontroller at virksomhedens sikkerhedsgodkendelse stadig gælder, og at der ved virksomheden ikke er ændret i forudsætningerne for godkendelsen, f.eks. fortsat en udpeget sikkerhedsansvarlig, fysiske sikkerhed for virksomhedens kontorer m.v., godkendte opbevaringsmidler, evt. godkendte IT-systemer osv. Virksomhedens sikkerhedsansvarlige kan evt. kontakte FE i tvivlstilfælde.

2. Kontroller medarbejderes status for personlig sikkerhedsgodkendelse (udløber normalt efter 2-5 år, eller hvis der sker ændringer i ansættelsesforhold, samlivsforhold, skift af bopæl m.m.)

3. Overvej om der ved en eventuel ordre fra DPS skal inddrages yderligere sikkerhedsgodkendte medarbejdere i virksomheden eller ved virksomhedens underleverandører. Tag eventuel kontakt til kontrakt- og indkøbsorganisationen ved DPS hovedleverandører (Terma A/S eller OMT) og få afklaret, om virksomhedens leverancer falder ind under klassificeret information. Hovedreglen er, at alt der kan afsløre patruljeskibets operative kapaciteter eller eventuelle sårbarheder overfor våbenanvendelse eller spionage, vil blive betragtet som klassificeret information.

4. Ansøgning om fornyelse af medarbejderes sikkerhedsgodkendelse eller for sikkerhedsgodkendelse af nye medarbejdere kan ske løbende og med direkte henvendelse via virksomhedens sikkerhedsansvarlig til FE.

3 HAR VIRKSOMHEDEN IKKE EN SIKKERHEDSGODKENDELSE UDSTEDT AF FE

I Patruljeskibsprojektet er det kun DPS, der kan indstille en virksomhed til sikkerhedsgodkendelse, og som udgangspunkt kan en ansøgning om sikkerhedsgodkendelse af virksomheden først finde sted, når man har modtaget en konkret ordre fra DPS eller er udpeget af særlige grunde, f.eks. en forventning om tilbudsindhentning af hastende karakter.

I langt de fleste tilfælde vil man som leverandør ikke have behov for sikkerhedsgodkendelse. DPS har altid mulighed for at ekstrahere klassificerede oplysninger fra specifikationer og kontrakter, så leverandøren stadig kan løse sin opgave uden at kende det samlede system eller skibets operative kapaciteter.

3.1 Proces for virksomhedens sikkerhedsgodkendelse

Processen starter med en vurdering af virksomhedens opgaver i relation til Patruljeskibsprojektet. Kræver det en sikkerhedsgodkendelse eller ej. DPS kerneleverandører (OMT hhv. Terma A/S) foretager denne vurdering i dialog med den konkrete virksomhed, hvor det afklares hvornår en sikkerhedsgodkendelse tidsmæssigt skal være på plads, eller om der slet ikke er behov for sikkerhedsgodkendelse. Da der trods alt forventes behov for sikkerhedsgodkendelse af et antal danske virksomheder, vil DPS prioritere de mest akutte leverancer og i første omgang indstille disse virksomheder til sikkerhedsgodkendelse. Som forberedelse til sikkerhedsgodkendelse anbefales følgende:

1. Tag eventuel kontakt til kontrakt- og indkøbsorganisationen ved DPS hovedleverandører (Terma A/S eller OMT) og få afklaret, om virksomhedens leverancer falder ind under klassificeret information. Hovedreglen er, at alt der kan afsløre patruljeskibets operative kapaciteter eller eventuelle sårbarheder overfor våbenanvendelse eller spionage, vil blive betragtet som klassificeret information.

2. Forbered eventuelle medarbejdere på udfyldelse af formular for ansøgning om sikkerhedsgodkendelse. Ansøgninger kan først fremsendes, når DPS har prioriteret virksomheden og notificeret FE herom.

3. Udfyld ansøgningsskema for virksomheden og send den til den enten Terma A/S eller OMT.

3.2 Ansøgningsproces for personlige sikkerhedsgodkendelser

I mange situationer leverer virksomheder ydelser i form af rådgivning, beregninger, analyser m.m. til en hovedleverandør, der allerede har sikkerhedsgodkendelse og sikkerhedsgodkendte medarbejdere. I sådanne situationer kan det være tilstrækkeligt, at de pågældende medarbejdere fra den rådgivende virksomhed bliver sikkerhedsgodkendte. I så fald arbejder rådgiveren i fortrolighed for hovedleverandøren (primært Terma A/S eller OMT), og den hovedleverandør kan initiere en sikkerhedsgodkendelse af den pågældende person, som var det en af hovedleverandørens egne medarbejdere. Samtidigt stiller hovedleverandøren krav til, hvor og hvordan rådgiveren skal arbejde, og hvordan afledte produkter skal håndteres.

Samtidigt med (eller i umiddelbar forlængelse af) fremsendelse af ansøgningsskema for virksomhedssikkerhedsgodkendelse jf. forrige afsnit bør der ansøges om sikkerhedsgodkendelse (som regel til klassifikationsgraden TIL TJENESTEBRUG) for den eller de medarbejdere, virksomheden udpeger for løsning af opgaven i relation til patruljeskibsprojektet. Som minimum skal virksomheden ansøge om sikkerhedsgodkendelse for virksomhedens leder og for den udpegede sikkerhedsansvarlige ved virksomheden. Hvis virksomheden er ledet af en bestyrelse, stilles der som regel også krav om, at bestyrelsesformanden sikkerhedsgodkendes og i visse tilfælde også andre medlemmer af bestyrelsen.

4 GODE RÅD, GENERELT

- Udvis altid diskretion med det eventuelle engagement med DPS. Offentliggørelse af kontrakter eller samarbejde med Forsvaret eller DPS skal godkendes inden frigivelse.
- For alle medarbejdere og for eventuelle underleverandører er det god stil aldrig at tale åbent om opgaver i relation til de nye patruljeskibe. Dette gælder også sociale medier.
- At udføre opgaver for Forsvaret stiller krav om ekstra forsigtighed og opmærksomhed fra både medarbejdere og virksomhedens ledelse. Spionage truslen er meget høj, især på højteknologiske områder og generelt inden for våben og sensorsystemer.
- Påbegynd uddannelse i sikkerhedsforståelse for medarbejdere tidligt. Der findes mange gode online undervisningsprogrammer, som forbereder medarbejderen på truslen og giver gode råd om rigtig adfærd, - især på IT-systemer.
- Den internationale standard ISO 27001/2 og/eller NIST SP 800-171 giver gode råd til virksomhedens informationssikkerhed.
- Alle opkoblinger af virksomhedens informationssystemer til Internettet udgør en potentiel risiko og vil som udgangspunkt ikke være tilladt, hvis der skal behandles klassificerede oplysninger.
- I begrænset omfang kan FMI/DPS midlertidigt stille godkendt PC-udstyr (laptop) til rådighed for virksomheder, hvis klassificerede informationer skal fremsendes til og behandles af virksomheden. Alternativt skal klassificerede dokumenter foreligge i fysisk form (papir eller lagermedie) og håndteres efter reglerne i FKOBST 358-1. Der gælder regler for både forsendelse og opbevaring, samt behandling og destruktion. En forudsætning er i øvrigt at person(erne) ved virksomheden, der skal modtage og behandle informationerne, er sikkerhedsgodkendt til den aktuelle klassifikationsgrad.
- Når virksomheden skal håndtere klassificeret information, skal man bruge ”Need-to-know” princippet og ikke ”Nice-to-know”. ”Need-to-know” betyder, at kun de medarbejdere, der har brug for det for at løse deres opgave, får adgang til de klassificerede informationer
- Som leverandør til DPS må virksomheden ikke viderefordele klassificeret materiale til andre, f.eks. underleverandører, uden først at have indhentet tilladelse fra DPS.
- Kommer klassificeret materiale i hænderne på uvedkommende eller er der opstået risiko herfor, skal dette straks rapporteres til FE og til DPS. Herudover kan der i visse tilfælde også være krav om at orientere Center for Cybersikkerhed ved Forsvarsministeriets Materiel- og indkøbsstyrelse (FMI).

5 NYTTIGE LINKS:

FE Risikovurdering:

https://www.fe-ddis.dk/da/produkter/Risikovurdering/

Center for Cyber Security trusselsvurdering:

https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/

Skemaer til sikkerhedsgodkendelse:

https://www.fe-ddis.dk/da/arbejdsomrade-a/Militaersikkerhed/skemaer-til-sikkerhedsgodkendelse/

Forsvarets sikkerhedsbestemmelser FKOBST 358-1:

https://www.fe-ddis.dk/globalassets/fe/dokumenter/fkobst-358-1/fkobst-358-1-filer/-fkobst-358-1-.pdf

FE vejledning om sikkerhedsgodkendelse:

https://www.fe-ddis.dk/da/arbejdsomrade-a/Militaersikkerhed/sikkerhedsgodkendelser/

FE vejledning om virksomhedssikkerhedsgodkendelse:

-vejlvirksik-2.30-.pdf (fe-ddis.dk)