Bilag 15

ISO27001 efterlevelse

|  |
| --- |
| ***Vejledning til tilbudsgiver***  *Bilaget indeholder et* ***mindstekrav*** *til Leverandørens risikostyring i forbindelse med de opgaver, der udføres under Rammekontrakten.*  *Bilaget består også af en række konkurrenceparametre, benævnt K1-Kn. For hvert af parametrene skal Leverandøren beskrive, hvordan Leverandøren opfylder de specifikke parametre, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.*  *Beskrivelserne skal indskrives i skemaet i punkt 3 og indgår i tilbudsevalueringen under kriteriet ”Kvalitet i opgaveløsningen”.* |

Indholdsfortegnelse

[1. Indledning 4](#_Toc506383383)

[2. Generelle mindstekrav til informationssikkerheden 4](#_Toc506383384)

[3. Specifikke konkurrenceparametre til Leverandørens ISMS 4](#_Toc506383385)

##### Indledning

Dette bilag omhandler Kundens mindstekrav og en række konkurrenceparametre til Leverandørens ledelsessystem for informationssikkerhedsstyring (ISMS) efter den til enhver tid gældende version af ISO/IEC 27001 eller tilsvarende (national eller international) anerkendt standard baseret på en risikostyringsproces.

Leverandøren er i hele kontraktperioden ved udførelse af opgaver omfattet af Rammekontrakten samt i forbindelse med overdragelse af Løsningen til en anden leverandør forpligtiget til at overholde parametrene i dette bilag som beskrevet af Leverandøren.

##### Generelle mindstekrav til informationssikkerheden

*MK-1*:Leverandøren skal opfylde de generelle krav til sikring af informationssikkerheden, som er beskrevet i punkt 14 vedr. sikkerhed i Rammekontrakten.

##### Specifikke konkurrenceparametre til Leverandørens ISMS

Baseret på Kundens risikovurdering af Løsningen og Kundens Statement of Applicability (SoA) i relation til Kundens ISMS, har Kunden identificeret en række specifikke parametre vedrørende Leverandørens ISMS, som Kunden vurderer, er særligt vigtige for at fastholde en høj it-sikkerhed i relation til Løsningen. Det skal bemærkes, at opfyldelse af parametrene nedenfor ikke er tilstrækkeligt til at opfylde MK-1 og de generelle krav, som er indeholdt i Rammekontraktens punkt 14.

For hvert af de nedenstående specifikke parametre til Leverandørens ISMS bedes Leverandøren beskrive, hvordan Leverandøren opfylder de specifikke parametre, medmindre parameteret *slet ikke* opfyldes eller opfyldes *fuldt ud*.

Hvis et parameter *slet ikke* opfyldes eller opfyldes *fuldt ud* angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.

Ved angivelse af fuld opfyldelse kan Kunden på ethvert tidspunkt bede om dokumentation herfor.

Det fremgår af udbudsbetingelsernes afsnit 7.2.4, at det vægter positivt, hvis parametrene opfyldes fuldt ud, og at det trækker ned i vurderingen, hvis tilbudsgiver slet ikke opfylder et parameter eller kun delvist opfylder et parameter.

**Tabel 1. Relevante parametre til leverandørens styring af sin it-sikkerhed baseret på ISO27001, anneks A.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter ID** | **Parametertekst baseret på ISO27001, anneks A** | **ISO27001 inputkilde** | **Leverandørens beskrivelse af sin opfyldelse** |
| **Styring af aktiver** | | | |
| *K-1* | Leverandøren skal identificere de Informationsaktiver, der anvendes til Kontraktens opfyldelse, og udarbejde og vedligeholde en elektronisk fortegnelse over disse Informationsaktiver. Leverandøren skal herunder dokumentere Systemet i overensstemmelse med Bilag 7 Dokumentation. | 8.1.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-2* | Leverandøren skal udpege personer og/eller entiteter hos Leverandøren som ejere af hvert Informationsaktiv, der anvendes til Kontraktens opfyldelse. Ejerskabet skal fremgå af den elektroniske fortegnelse, jf. K-18. | 8.1.2 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-3* | Leverandøren skal sikre, at alle Leverandørens medarbejdere afleverer alle Informationsaktiver, som har været anvendt til Kontraktens opfyldelse, og som er i deres besiddelse, når deres ansættelse eller aftale ophører. | 8.1.4 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Adgangsstyring** | | | |
| *K-4* | Leverandøren skal fastlægge, dokumentere og vedligeholde en politik for adgangsstyring i relation til Kontraktens opfyldelse i overensstemmelse med den til enhver tid gældende risikovurdering, jf. punkt 14 i Rammekontrakten. | 9.1.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-5* | Leverandøren skal sikre, at Brugere og Leverandørrens medarbejdere kun har adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte i relation til Kontraktens opfyldelse, jf. også K-4. | 9.1.2 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Administration af brugeradgang** | | | |
| *K-6* | Leverandøren skal implementere en formel procedure for registrering og afmelding af Brugere med henblik på tildeling af adgangsrettigheder i forbindelse med Kontraktens opfyldelse. | 9.2.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-7* | Leverandøren skal implementere en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester, der anvendes til Kontraktens opfyldelse. | 9.2.2 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-8* | Leverandøren skal sikre, at aktivejere med jævne mellemrum gennemgår Leverandørens medarbejderes adgangsrettigheder og autorisationer i relation til Kontraktens opfyldelse. | 9.2.5 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-9* | Leverandøren skal inddrage alle medarbejderes og eksterne brugeres adgangsrettigheder og autorisationer til information og informationsbehandlingsfaciliteter i relation til Kontraktens opfyldelse, når deres ansættelsesforhold, kontrakt eller aftale ophører eller skal tilpasses efter en ændring. | 9.2.6 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Brugerens ansvar** | | | |
| *K-10* | Leverandøren skal begrænse adgangen til information og applikationssystemers funktioner i relation til Kontraktens opfyldelse i overensstemmelse med politikken for adgangsstyring, jf. K-5 | 9.4.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-11* | Adgang til systemer og applikationer, der anvendes til Kontraktens opfyldelse, skal styres af en procedure for sikker log-on i overensstemmelse med politikken for adgangsstyring, jf. K-4 | 9.4.2 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-12* | Leverandøren skal sikre, at systemer til administration af adgangskoder i relation til Kontraktens opfyldelse er interaktive og sikrer adgangskoder af høj kvalitet | 9.4.3 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Udstyr** | | | |
| *K-13* | Leverandøren skal sikre, at udstyr, der anvendes til Kontraktens opfyldelse, placeres og beskyttes, således at risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes. Placering og beskyttelse af udstyr skal afspejle den gældende risikovurdering, jf. Rammekontraktens punkt 14. | 11.2.1 | *[Leverandøren skal angive, om Leverandøren lever fuldt ud, delvist eller slet ikke op til parameteret.*  *Leverandøren skal beskrive sin opfyldelse såfremt Leverandøren kun delvist opfylder parameteret.]* |
| **Malwarebeskyttelse** | | | |
| *K-14* | Leverandøren skal i relation til Kontraktens opfyldelse implementere kontroller til detektering, forhindring og gendannelse for at beskytte mod malware i kombination med passende brugerbevidsthed. De pågældende procedurer og værktøjer skal afspejle den gældende risikovurdering, jf. Rammekontraktens punkt 14. | 12.2.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Backup** | | | |
| *K-15* | Leverandøren skal sikre, at der tages backupkopier af information, Programmel og system-images, der anvendes af Leverandøren til Kontraktens opfyldelse, og disse skal testes regelmæssigt i overensstemmelse med den aftalte backuppolitik. | 12.3.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Logning og overvågning** | | | |
| *K-16* | Leverandøren skal sikre, at hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser i relation til Kontraktens opfyldelse udføres, opbevares og gennemgås regelmæssigt. | 12.4.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Sårbarhedsstyring** | | | |
| *K-17* | Leverandøren skal som led i sin risikovurdering, jf. Rammekontraktens punkt 14, have en dokumenteret proces for løbende indhentning af informationer om aktuelle tekniske sårbarheder i Løsningen. Leverandøren skal såfremt de bliver opmærksomme på tekniske sårbarheder i Løsningen, som kan have betydning for informationssikkerheden i systemet, orientere Kunden. Leverandøren skal rådgive Kunden om passende foranstaltninger til at håndtere den tilhørende risiko. | 12.5.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Sikkerhed i udviklings- og hjælpeprocesser** | | | |
| *K-18* | Leverandøren skal styre ændringer af Programmel inden for udviklingslivscyklussen, som Leverandøren anvender til Kontraktens opfyldelse, ved hjælp af formelle procedurer for ændringsstyring. | 14.2.2 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-19* | Leverandøren skal gennemgå og teste Applikationer, der er forretningskritiske for Kontraktens opfyldelse, ved ændring af Infrastrukturen for at sikre, at ændringen ikke indvirker negativt på drift og sikkerhed. | 14.2.3 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-20* | Leverandøren skal sikre, at principper for udvikling af sikre systemer fastlægges, dokumenteres, opretholdes og anvendes i forbindelse med de implementeringer af informationssystemer, som Leverandøren anvender i relation til Kontraktens opfyldelse. | 14.2.5 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| *K-21* | Leverandøren skal udføre test af sikkerhedsfunktionalitet ved systemudvikling relateret til Kontraktens opfyldelse. | 14.2.8 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Informationssikkerhed i leverandørforhold** | | | |
| *K-22* | Leverandøren skal sikre, at informationssikkerhedskrav til at minimere risici forbundet med underleverandørers adgang til Informationsaktiver, der anvendes til Kontraktens opfyldelse, aftales med underleverandører og dokumenteres. Leverandøren skal herunder sikre, at informationssikkerhedskravene til underleverandøren er passende henset til den gældende risikovurdering, jf. Rammekontraktens punkt 14. | 15.1.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |
| **Styring af informationssikkerhedsbrud og forbedringer** | | | |
| *K-23* | Leverandøren skal fastlægge ledelsesansvar og procedurer for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud relateret til Kontraktens opfyldelse. | 16.1.1 | *[Leverandøren skal beskrive, hvordan Leverandøren opfylder parameteret, medmindre parameteret slet ikke opfyldes eller opfyldes fuldt ud.*  *Hvis et parameter slet ikke opfyldes eller opfyldes fuldt ud angives dette, og der skal ikke fremgå yderligere beskrivelse af parameteret.]* |