KONKURRENCE- OG FORBRUGERSTYRELSEN

Bilag 15. ISO27001 efterlevelse

Vejledning til tilbudsgiver

*Hele bilaget udgør et **mindstekrav**. Bilaget skal ikke udfyldes som en del af tilbudsafgivelsen.*

Indholdsfortegnelse

1. Indledning

Dette bilag omhandler Kundens mindstekrav 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 kravene i dette bilag.

2. 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.

3. Specifikke mindstekrav 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 mindstekrav 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 mindstekravene nedenfor ikke er tilstrækkeligt til at opfylde MK-1 og de generelle krav, som er indeholdt i Rammekontraktens punkt 14.

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

Krav-ID	Mindstekrav baseret på ISO27001, anneks A	ISO27001 inputkilde
Sikkerhedskrav under ansættelsen – ISO27001, Anneks A, punkt 7.2		
MK-2	Leverandøren skal sikre, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer i relation til Kontraktens opfyldelse.	7.2.1
Ansvar for aktiver – ISO27001, Anneks A, punkt 8.1		
MK-3	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
MK-4	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. MK-18.	8.1.2
MK-5	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

Forretningsmæssige krav til adgangsstyring – ISO27001, Anneks A, punkt 9.1		
MK-6	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

Administration af brugeradgang – ISO27001, Anneks A, punkt 9.2.		
MK-7	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
MK-8	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
MK-9	Leverandøren skal sikre, at aktivejere med jævne mellemrum gennemgår Leverandørens medarbejderes adgangsrettigheder og autorisationer i relation til Kontraktens opfyldelse.	9.2.5
MK-10	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

Malwarebeskyttelse – ISO27001, Anneks A, punkt 12.2		
MK-11	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

Backup – ISO27001, Anneks A, punkt 12.3		
MK-12	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
Logning og overvågning – ISO27001, Anneks A, punkt 12.4		
MK-13	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

Sårbarhedsstyring – ISO27001, Anneks A, punk 12.6		
MK-14	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
Overvejelser i forbindelse med audit af informationssystemer – ISO27001, Anneks A, punkt 12.7		
MK-15	Leverandøren skal sikre, at auditkrav og -aktiviteter i relation til Kontraktens opfyldelse, der indebærer verificering af driftssystemer, planlægges og aftales omhyggeligt for at minimere afbrydelser af Kundens forretningsprocesser.	12.7.1

Sikkerhed i udviklings- og hjælpeprocesser – ISO27001, Anneks A, punkt 14.2.		
MK-16	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
MK-17	Leverandøren skal gennemgå og teste Applikationer, der er forretningskritiske for Kontraktens opfyldelse, når Leverandøren får information fra Kunden eller Statens IT om ændring af Infrastrukturen for at sikre, at ændringen ikke indvirker negativt på drift og sikkerhed.	14.2.3
MK-18	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

Informationssikkerhed i leverandørforhold – ISO27001, Anneks A, punkt 15.1		
MK-19	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

Styring af informationssikkerhed og forbedringer – ISO27001, Anneks A, punkt 16.1		
MK-20	Leverandøren skal fastlægge ledelsesansvar og procedurer for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud relateret til Kontraktens opfyldelse.	16.1.1
MK-21	Leverandøren skal sikre, at informationssikkerhedshændelser relateret til Kontraktens opfyldelse rapporteres ad passende ledelseskanaler så hurtigt som muligt.	16.1.2
MK-22	Leverandøren skal sikre, at medarbejdere og kontrahenter, som bruger informationssystemer og -tjenester, der anvendes til Kontraktens opfyldelse, har pligt til at notere og rapportere alle observerede svagheder eller mistanker om svagheder i disse informationssystemer og -tjenester.	16.1.3
Overensstemmelse med lov og kontrakkrav – ISO27001, Anneks A, punkt 18.1		
MK-23	Leverandøren skal sikre, at alle relevante lov-, myndigheds- og kontraktkrav, samt Leverandørens metode til overholdelse af disse krav, er klart identificeret, dokumenteret og opdateret for hvert informationssystem og for Leverandørens organisation.	18.1.1
MK-24	Leverandøren skal sikre, at privatlivets fred og personoplysninger i relation til Kontraktens opfyldelse beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter.	18.1.4