Aarhus Universitet

Bilag 12 - Sikkerhed

Drift af Oracle SOA-platform

Aarhus Universitet

Indholdsfortegnelse

1. INDLEDNING

Dette bilag indeholder Kundens krav til sikkerhed og Leverandørens opfyldelse heraf.

2. GENERELLE SIKKERHEDSKRAV

K-1 Ledelsessystem for informationssikkerhedsstyring

Leverandøren skal med henblik på løbende sikring af informationssikkerhed i tilknytning til levering af Ydelserne opretholde et ledelsessystem for informationssikkerhedsstyring (ISMS) efter den til enhver tid gældende version af ISO27001 eller tilsvarende (national eller international) anerkendt standard baseret på en risikostyringsproces, jf. K-2, og i overensstemmelse med de i punkt 3 angivne specifikke krav til Leverandørens ISMS. Leverandøren skal herunder løbende tilpasse sit ISMS, såfremt Leverandørens opdatering af sin risikovurdering, jf. K-2, medfører et behov herfor.

K-2 Risikovurdering

Leverandørens risikostyring af informationssikkerheden i forhold til Leverandørens opfyldelse af Kontrakten skal baseres på en dokumenteret og regelmæssigt opdateret risikovurdering. I relation til Leverandørens risikovurdering gælder det, at:

- Risikovurderingen skal omfatte de Ydelser og de dele af Leverandørens virksomhed, som kan have konsekvenser for informationssikkerheden i Systemet,
- Leverandøren som minimum skal opdatere sin risikovurdering én (1) gang årligt, samt i forbindelse med forestående ændringer af Leverandørens egne organisatoriske forhold, forestående ændringer af en eventuel underleverandørs forhold eller forestående ændringer af Systemet, der erfaringsmæssigt kan have konsekvenser for informationssikkerheden for de med Kontrakten forbundne Ydelser,
- Leverandøren skal opdatere sin risikovurdering efter påbud fra Kunden om at inkludere en specifik trussel i risikovurderingen, herunder men ikke begrænset til som følge af ændringer i Kundens egen til enhver tid gældende risikovurdering og/eller konsekvensanalyse vedrørende databeskyttelse (DPIA). En sådan af Kunden påbudt opdatering af Leverandørens risikovurdering skal ske inden for en passende frist henset til truslens karakter, samt at
- Leverandøren uden ugrundet ophold skal fremsende Leverandørens gældende risikovurdering med henblik på Kundens godkendelse, og således at Kunden til enhver tid har Leverandørens seneste risikovurdering.

3. SPECIFIKKE SIKKERHEDSKRAV

K-3 *Kundens sikkerhedspolitikker*

Leverandørens medarbejdere skal overholde Kundens til enhver tid gældende; politikker og instrukser, herunder it- og sikkerhedspolitikker, Kundens krav til og retningslinjer for sikkerhedsforhold, metoder, processer, værktøjer og standarder, samt Kundens interne regler for f.eks. adgangskontrol, insiderviden, intern revision, mv., som de til enhver tid gælder for Kundens øvrige medarbejdere. Kunden skal løbende holde Leverandøren orienteret om ændringer til disse regler.

K-4 *Leverandørens sikkerhedspolitikker*

Leverandøren skal inden indgåelse af Kontrakten fremsende dokumentation for Leverandørens sikkerhedsniveau og sikkerhedspolitik.