



Aarhus Universitet

## Bilag 4.e – Revision og kontrol

Drift af Security Operations Centre (SOC)



## Indholdsfortegnelse

|     |                                                                                |   |
|-----|--------------------------------------------------------------------------------|---|
| 1.  | INDLEDNING.....                                                                | 3 |
| 2.  | KRAV TIL REVISION OG KONTROL .....                                             | 3 |
| 2.1 | Revision og kontrol med Leverandørens opfyldelse af kravene til sikkerhed..... | 3 |



## 1. INDLEDNING

Dette bilag indeholder Kundens krav til den revision og kontrol af Leverandørens Ydelser, som Leverandøren skal levere under Kontrakten.

## 2. KRAV TIL REVISION OG KONTROL

### 2.1 Revision og kontrol med Leverandørens opfyldelse af kravene til sikkerhed

#### *K-1 Informationssikkerhed*

Leverandøren skal senest seks måneder efter Transitionsdagen og herefter hver 12. måned kunne fremvise en opdateret ledelseserklæring vedrørende Kontraktens krav til sikkerhed.

Denne ledelseserklæring skal omfatte:

- a. Dokumentation for Leverandørens efterlevelse af kravene i relation til Leverandørens ledelsessystem for informationssikkerhedsstyring, jf. Bilag 12 (Sikkerhed), K-1. Leverandøren kan opfylde sin dokumentationsforpligtelse ved levering af et gyldigt ISO27001-certifikat eller tilsvarende certifikat, i det omfang Leverandøren kan påvise, at pågældende certificering dokumenterer opfyldelsen af Kundens krav i relation til Leverandørens ledelsessystem for informationssikkerhedsstyring, jf. Bilag 12 (Sikkerhed), K-1

Denne ledelseserklæring skal omfatte mindst en af følgende:

- b. En uafhængig revisors ISAE 3000-erklæring (eller tilsvarende revisionserklæring typegodkendt af Kunden), der afgives med en høj grad af sikkerhed for perioden siden seneste revisionserklæring, om kontroller rettet mod Leverandørens overholdelse af Kontraktens krav til sikkerhed, jf. Bilag 12 (Sikkerhed)
- c. En uafhængig revisors ISAE 3402, type II-erklæring (eller tilsvarende revisionserklæring typegodkendt af Kunden), der afgives med en høj grad af sikkerhed for perioden siden seneste revisionserklæring, for forhold og faciliteter hos Leverandøren, der deles med Leverandørens øvrige Kunder, og som har betydning for informationssikkerheden i relation til Kontraktens opfyldelse.

#### *K-2 Udgifter forbundet med Revision og Kontrol*

Leverandøren afvikler selv udgifter til Revision og Kontrol, herunder revisionserklæringer og efterlevelse af ISO 27001.