| Bilag 14 - Sikkerhed |
| --- |

[Projektnavn]

[Måned + år]

[**Vejledning til Kunden**

Vejledning til Kunden er angivet i skarpe parenteser og markeret med gult. Udover denne generelle vejledning kan standardbilaget indeholde specifikke vejledninger til kunden.

Dette standardbilag er et kategori B-bilag. Kategori B betyder, at standardbilaget er *delvist* færdiggjort, og i de fleste konkrete kontrakter skal færdiggøres af Kunden for at være dækkende for Kundens behov.

Ved udarbejdelsen af dette bilag er der taget udgangspunkt i Digitaliseringsstyrelsens vejledning ”*Sådan stiller du krav til leverandører om informationssikkerhed –* *Katalog*”, fra december 2017. Vejledningen kan findes her: [”Sådan stiller du krav til leverandører om informationssikkerhed – Katalog” på Digst.dk](https://digst.dk/styring/standardkontrakter/klausuler-til-informationssikkerhed/kravkatalog-til-leverandoerer/" \o "#AutoGenerate)

Med henblik på at understøtte en risikobaseret tilgang til informationssikkerhed er der ved udarbejdelsen af dette standardbilag indarbejdet de ”generelle krav” til informationssikkerhed fra ovennævnte vejledning. Se dette bilag 14, punkt 2. Det er forudsat, at kunden i tillæg til de generelle krav implementerer sine konkrete krav til sikkerhed. I standardbilagets opbygning er det forudsat, at kundens konkrete krav implementeres i punkt 3.

Det anbefales, at der stilles krav om Leverandørens forpligtelse til at dokumentere opfyldelsen af de stillede krav til sikkerhed. Eksempler på sådanne krav findes i Bilag 4.e (Revision og kontrol).

Såfremt Kontrakten er omfattet af de udbudsretlige regler, skal bilaget endvidere tilpasses i overensstemmelse hermed. Dette vil ofte indebære, at bilaget og vejledning til leverandøren skal afstemmes med udbuddets udbudsbetingelser, der beskriver udbudsprocessen og rammerne for konkurrencen.

Vejledning til Kunden bør slettes inden kontraktmaterialet offentliggøres.]

*[****Vejledning til leverandøren***

*Vejledning til leverandøren er angivet med kursiv i skarpe parenteser som denne. Udover denne generelle vejledning indeholder bilaget en række specifikke vejledningstekster til leverandøren.*

*Leverandøren skal udfylde dette Bilag 14 i overensstemmelse med den specifikke vejledning herom og indleveres som en del af tilbuddet.*

*Leverandøren skal desuden udfylde kravmatricen sidst i bilaget.*

*Leverandøren skal ikke ændre i bilaget, medmindre dette specifikt er angivet i vejledning til leverandøren, eller hvor det er markeret på anden vis.*

*I Kontrakten er der henvist til Bilag 14, Sikkerhed i følgende punkter:*

* *Punkt 33 (Sikkerhed)*

*Vejledning til leverandøren slettes inden kontraktunderskrift.]*

1. Indholdsfortegnelse

[1. Indledning 5](#_Toc517166802)

[2. Generelle sikkerhedskrav 5](#_Toc517166803)

[3. Specifikke sikkerhedskrav 6](#_Toc517166804)

[4. KRAVMATRICE 7](#_Toc517166805)

# Indledning

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

# Generelle sikkerhedskrav

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.

1. 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.

# Specifikke sikkerhedskrav

1. […]
2. […]

# KRAVMATRICE

[Kravmatricen skal færdiggøres konkret. Såfremt Kontrakten er omfattet af udbudsreglerne, skal matricen færdiggøres i overensstemmelse med de konkrete udbudsretlige beslutninger, herunder med udbuddets udbudsbetingelser, jf. også den generelle vejledning til kunden.]

***[Vejledning til leverandøren:***

*Leverandøren skal udfylde kravmatricen med angivelse af graden, hvormed kravene i dette bilag er opfyldt.]*

| Krav ID | Udbudsretlig kravrubricering | Opfyldelsesgrad  (Helt /  Opfyldes delvist /  Opfyldes ikke) | Leverandørens beskrivelse eller reference til løsningsbeskrivelse i separat dokument |
| --- | --- | --- | --- |
| K-1 |  |  |  |
| K-2 |  |  |  |
| K-3 |  |  |  |
| K-4 |  |  |  |