Virksomhedsnavn	
Kunde	

Leverandørtype

Vi er leverandør af:

- ◯ Hardware (fx computere, tablet, printere, skærme og tastaturer)
- ◯ Hardware (fx netværksudstyr, switchere og routere)
- ◯ Software u. egen kodeudvikling (fx operativsystemer, databaser, programmeringsværktøjer og applikationssoftware)
- ◯ It/cybersikkerhed (fx antivirus, firewall og intrusion detection)
- ◯ It-infrastruktur (fx hosting og cloud computing)
- ◯ It-konsulentservices (fx it-rådgivning- og tjenester, systemudvikling, systemintegration og it-drift)
- ◯ It-uddannelse (fx kurser og certificeringer)
- ◯ Software m. egen kodeudvikling (fx operativsystemer, databaser, programmeringsværktøjer og applikationssoftware)
- ◯ Andet:

Risikoprofil

Vores risikoprofil er:

◯ **Ingen eller lav negativ effekt (ingen/begrænset adgang til kundens netværk mv.)**

Fra kundens perspektiv vil en leverandør med denne risikoprofil typisk have:

- Adgang til kun offentligt tilgængelige informationer
- Adgang til kun mindre aktiver
- Ingen adgang/forbindelse til organisationens netværk
- Ingen leverance af services, der er kritiske for forretningen

Cyberangreb eller databrud hos denne risikoprofil vurderes at kunne forårsage

- Ingen eller begrænset omdømmeskade
- Ingen eller begrænset indvirkning på forretningsdrift og/eller processer
- Ingen eller minimale økonomiske/juridiske konsekvenser

◯ **Moderat negativ effekt (adgang til netværk, data, større aktiver mv.)**

Fra kundens perspektiv vil en leverandør med denne risikoprofil typisk have:

- Adgang til oplysninger der indeholder personhenførbare data
- Adgang til større aktiver (kun standardadgang)
- Adgang/forbindelse til organisationens netværk
- Leverance af services, der kan have forstyrrende påvirkning af forretningen

Cyberangreb eller databrud hos denne risikoprofil vurderes at kunne forårsage

- En vis omdømmeskade
- En vis indvirkning på forretningsdrift og/eller processer
- Nogle økonomiske/juridiske konsekvenser

◯ **Stor negativ effekt (adgang til netværk med rettigheder, privilegeret adgang til følsomme data mv.)**

Fra kundens perspektiv vil en leverandør med denne risikoprofil typisk have:

- Privilegeret adgang til og mulighed for behandling af personhenførbare og/eller kommercielt følsomme data
- Privilegeret adgang til større eller forretningskritiske aktiver
- Adgang/forbindelse til organisationens netværk med yderligere rettigheder
- Leverance af services, der kan have kritisk påvirkning af forretningen

Cyberangreb eller databrud hos denne risikoprofil vurderes at kunne forårsage

- Høj omdømmeskade
- Stor indvirkning på forretningsdrift og/eller processer
- Høje økonomiske/juridiske konsekvenser

IT·BRANCHEN

Tekniske minimumsforanstaltninger

Risikoprofil 1 (Ingen eller lav negativ effekt)

	Implementeret	Igang	Mangler
● Dokumenteret overblik over vigtige data og systemer			
● Opdatering af operativsystemer og applikationer			
● Antivirus og firewall på alle systemer, klienter og online indgange			
● Beskyttet og testet backup af forretningskritiske systemer og data			
● Fokus på at kunne spotte mistænkelige mails og links, inklusiv awareness-træning			
● Politik for lange og unikke passwords, brug af password manager og to-faktor validering			

Risikoprofil 2 (Moderat negativ effekt)

Implementering af ovenstående minimumskrav +	Implementeret	Igang	Mangler
● Defineret og implementeret cyber- og informationssikkerhedspolitik			
● Udpeget it-sikkerhedsansvarlig			
● Defineret og testet beredskabsplan			
● Udvidet awareness-træning af ledelse og medarbejdere			
● Adgangskontrol og rettighedsstyring			
● Beskyttet fjernadgang til systemer (kryptering og flerfaktor-autentifikation)			
● Fysisk sikring af in-infrastruktur, systemer, klienter og data			

Risikoprofil 3 (Stor negativ effekt)

Implementering af ovenstående minimumskrav +	Implementeret	Igang	Mangler
● Dokumenteret proces for risikostyring			
● Sårbarhedsscanning			
● Politik eller anvendt standard for beskyttelse af OT (hvis relevant)			
● Netværkssegmentering			
● Logning og monitorering			
● Konfigurationsstyring			
● Styr på anskaffelse, vedligeholdelse og bortskaffelse af informationsaktiver			
● Grundlæggende viden om cybersikkerhed og ansvarlig dataanvendelse hos ledelse, medarbejdere og kritiske underleverandører			
● Krav til og tilsyn med cybersikkerheden hos kritiske underleverandører			
● Metode/kanal for rapportering af sårbarheder på produkter fra tredjepart			
● Politik eller anvendt standard for sikkerhed i kodeudvikling (hvis relevant)			

IT·BRANCHEN