

Virksomhedsnavn	
Kunde	
Leverandørtype	<p>Vi er leverandør af:</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <ul style="list-style-type: none"> <input type="radio"/> Hardware (fx computere, tablet, printere, skærme og tastaturer) <input type="radio"/> Hardware (fx netværksudstyr, switchere og routere) <input type="radio"/> Software u. egen kodeudvikling (fx operativsystemer, databaser, programmeringsværktøjer og applikationssoftware) <input type="radio"/> It/cybersikkerhed (fx antivirus, firewall og intrusion detection) <input type="radio"/> It-infrastruktur (fx hosting og cloud computing) </div> <div style="width: 48%;"> <ul style="list-style-type: none"> <input type="radio"/> It-konsulentstjenester (fx it-rådgivning- og tjenester, systemudvikling, systemintegration og it-drift) <input type="radio"/> It-uddannelse (fx kurser og certificeringer) <input type="radio"/> Software m. egen kodeudvikling (fx operativsystemer, databaser, programmeringsværktøjer og applikationssoftware) <input type="radio"/> Andet: </div> </div>
Risikoprofil	<p>Vores risikoprofil er:</p> <ul style="list-style-type: none"> <input type="radio"/> Ingen eller lav negativ effekt (ingen/begrænset adgang til kundens netværk mv.) <i>Fra kundens perspektiv vil en leverandør med denne risikoprofil typisk have:</i> <ul style="list-style-type: none"> • Adgang til kun offentligt tilgængelige informationer • Adgang til kun mindre aktiver • Ingen adgang/forbindelse til organisationens netværk <i>Cyberangreb eller databrud hos denne risikoprofil vurderes at kunne forårsage</i> <ul style="list-style-type: none"> • Ingen eller begrænset omdømmeskade • Ingen eller begrænset indvirkning på forretningsdrift og/eller processer • Ingen eller minimale økonomiske/juridiske konsekvenser <input type="radio"/> Moderat negativ effekt (adgang til netværk, data, større aktiver mv.) <i>Fra kundens perspektiv vil en leverandør med denne risikoprofil typisk have:</i> <ul style="list-style-type: none"> • Adgang til oplysninger der indeholder personhenførbare data • Adgang til større aktiver (kun standardadgang) • Adgang/forbindelse til organisationens netværk <i>Cyberangreb eller databrud hos denne risikoprofil vurderes at kunne forårsage</i> <ul style="list-style-type: none"> • En vis omdømmeskade • En vis indvirkning på forretningsdrift og/eller processer • Nogle økonomiske/juridiske konsekvenser <input type="radio"/> Stor negativ effekt (adgang til netværk med rettigheder, privilegeret adgang til følsomme data mv.) <i>Fra kundens perspektiv vil en leverandør med denne risikoprofil typisk have:</i> <ul style="list-style-type: none"> • 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 <i>Cyberangreb eller databrud hos denne risikoprofil vurderes at kunne forårsage</i> <ul style="list-style-type: none"> • Høj omdømmeskade • Stor indvirkning på forretningsdrift og/eller processer • Høje økonomiske/juridiske konsekvenser

Tekniske minimumsforanstaltninger

Risikoprofil 1 (Ingen eller lav negativ effekt)

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

Risikoprofil 2 (Moderat negativ effekt)

Implementering af ovenstående minimumskrav +

	Klaret	Igang	Mangler
● Defineret og implementeret cyber- og informationssikkerhedspolitik	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Udpeget it-sikkerhedsansvarlig	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Defineret og testet beredskabsplan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Udvidet awareness-træning af ledelse og medarbejdere	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Adgangskontrol og rettighedsstyring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Beskyttet fjernadgang til systemer (kryptering og flerfaktor-autentifikation)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Fysisk sikring af in-infrastruktur, systemer, klienter og data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Risikoprofil 3 (Stor negativ effekt)

Implementering af ovenstående minimumskrav +

	Klaret	Igang	Mangler
● Dokumenteret proces for risikostyring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Sårbarhedsscanning	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Politik eller anvendt standard for beskyttelse af OT (hvis relevant)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Netværkssegmentering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Logning og monitorering	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Konfigurationsstyring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Styr på anskaffelse, vedligeholdelse og bortskaffelse af informationsaktiver	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Grundlæggende viden om cybersikkerhed og ansvarlig dataanvendelse hos ledelse, medarbejdere og kritiske underleverandører	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Krav til og tilsyn med cybersikkerheden hos kritiske underleverandører	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Metode/kanal for rapportering af sårbarheder på produkter fra tredjepart	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>