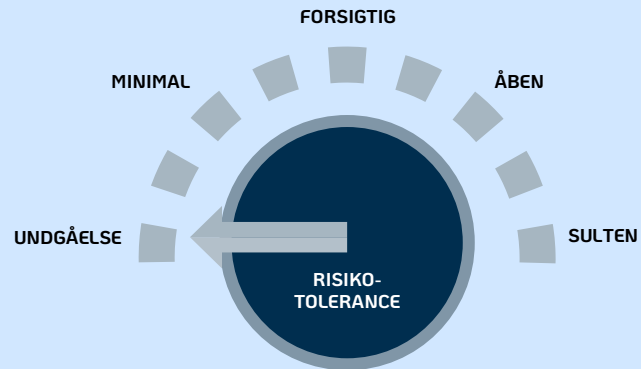


NÅR RISIKOTOLERANCEN ER 'UNDGÅELSE'



Villighed til at absorbere tab

	Fysiske hændelser	Eksterne ondsindede angreb (cyber)	Interne ondsindede angreb	Interne fejl og mangler	Hændelser fra outsourcing
5%	95.000	95.000	95.000	95.000	95.000
50%	50.000	50.000	50.000	50.000	50.000
95%	5.000	5.000	5.000	5.000	5.000

GENEREL BESKRIVELSE AF RISIKOTOLERANCEN

Vores mål er at sikre, at virksomheden opretholder den højst mulige it-sikkerhed.

Vi accepterer ingen risiko i forbindelse med beskyttelsen af it-systemer og data.

Vi accepterer ingen udvikling på de eksisterende løsninger.

RAPPORTERINGSGRÆNSER FOR ENKELTHÆNDELSER

Bestyrelsen skal orienteres om enhver hændelse på it-området uden unødigt ophold.

VILLIGHED TIL AT ABSORBERE TAB FRA IT-HÆNDELSER

Af tabellen til venstre fremgår risikotolerancen for hvert af de fem risikoområder.

Tallene læses som en villighed til et årligt tab med en vis sandsynlighed.

NÅR RISIKOTOLERANCEN ER 'MINIMAL'



Villighed til at absorbere tab

	Fysiske hændelser	Eksterne ondsindede angreb (cyber)	Interne ondsindede angreb	Interne fejl og mangler	Hændelser fra outsourcing
5%	95.000	500.000	195.000	195.000	195.000
50%	100.000	100.000	100.000	100.000	100.000
95%	10.000	10.000	10.000	10.000	10.000

GENEREL BESKRIVELSE AF RISIKOTOLERANCEN

Vores mål er at sikre, at virksomheden opretholder de højeste standarder for it-sikkerhed.

Vi accepterer minimal risiko i forbindelse med beskyttelsen af it-systemer og data.

Vi implementerer de mest stringente sikkerhedsforanstaltninger, udfører kontinuerlig overvågning og reagerer øjeblikkeligt på enhver potentiel trussel.

Vi forpligter os til at overholde alle relevante lovgivninger og bedste praksis inden for it-sikkerhed uden undtagelse.

Vi accepterer kun udvikling på de eksisterende løsninger så længe dette ikke medfører et højere risikoniveau for den samlede løsning.

RAPPORTERINGSGRÆNSER FOR ENKELTHÆNDELSER

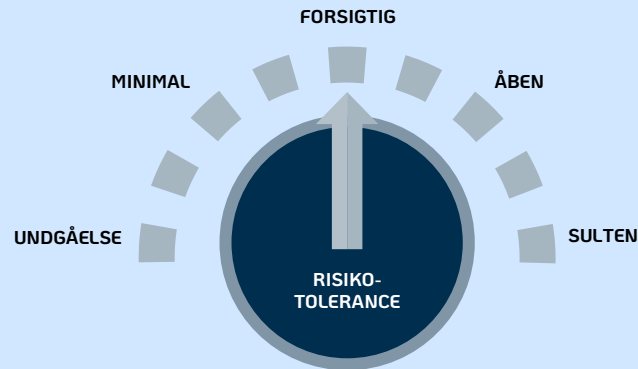
Bestyrelsen skal orienteres om hændelser uden unødigt ophold hvis tilgængeligheden er væsentligt forringet eller afbrudt i mere end 1 time.

Bestyrelsen skal orienteres om hændelser uden unødigt ophold hvis følsomme oplysninger i virksomheden bliver (eller formodes at være) tilgået af ondsindede eksterne aktører eller hvis hændelsen formodes at kunne resultere i nogen form for medieopmærksomhed.

VILLIGHED TIL AT ABSORBERE TAB FRA IT-HÆNDELSER

Af tabellen til venstre fremgår risikotolerancen for hvert af de fem risikoområder. Tallene læses som en villighed til et årligt tab med en vis sandsynlighed.

NÅR RISIKOTOLERANCEN ER 'FORSIGTIG'



Villighed til at absorbere tab

	Fysiske hændelser	Eksterne ondsindede angreb (cyber)	Interne ondsindede angreb	Interne fejl og mangler	Hændelser fra outsourcing
5%	500.000	1.000.000	500.000	500.000	500.000
50%	250.000	500.000	250.000	250.000	250.000
95%	100.000	20.000	100.000	100.000	100.000

GENEREL BESKRIVELSE AF RISIKOTOLERANCEN

Vores mål er at sikre, at virksomheden opretholder høje standarder for it-sikkerhed.

Vi stræber efter at beskytte selskaber og brugeres data gennem proaktive sikkerhedsforanstaltninger, kontinuerlig overvågning og hurtig respons på potentielle trusler.

Vi forpligter os til at overholde al relevant lovgivning og god praksis inden for it-sikkerhed. Vi ønsker samtidig at udvikle relevante digitale løsninger til vores kunder og brugere og accepterer ved den aktivitet en vis risiko.

RAPPORTERINGSGRÆNSER FOR ENKELTHÆNDELSER

Bestyrelsen skal orienteres om hændelser via de almindelige rytmer for rapportering hvis tilgængeligheden til virksomhedens systemer er væsentligt forringet eller afbrudt i mere end 4 timer.

Bestyrelsen skal orienteres om hændelser uden unødigt ophold hvis tilgængeligheden er væsentligt forringet eller afbrudt i mere end 8 timer.

Bestyrelsen skal orienteres om hændelser uden unødigt ophold hvis følsomme oplysninger i virksomheden bliver (eller formodes at være) tilgået af ondsindede eksterne aktører.

Bestyrelsen skal orienteres om hændelser uden unødigt ophold hvis hændelsen formodes at kunne resultere i medieopmærksomhed.

VILLIGHED TIL AT ABSORBERE TAB FRA IT-HÆNDELSER

Af tabellen til venstre fremgår risikotolerancen for hvert af de fem risikoområder. Tallene læses som en villighed til et årligt tab med en vis sandsynlighed.

NÅR RISIKOTOLERANCEN ER 'ÅBEN'



Villighed til at absorbere tab

	Fysiske hændelser	Eksterne ondsindede angreb (cyber)	Interne ondsindede angreb	Interne fejl og mangler	Hændelser fra outsourcing
5%	1.000.000	5.000.000	1.000.000	1.000.000	1.000.000
50%	500.000	1.000.000	500.000	500.000	500.000
95%	250.000	250.000	250.000	250.000	250.000

GENEREL BESKRIVELSE AF RISIKOTOLERANCEN

Vores mål er at sikre, at virksomheden opretholder en vis grad af it-sikkerhed, samtidig med at vi er åbne for at tage betydelige risici for at fremme innovation og udvikling.

Vi er villige til at acceptere en høj grad af risiko i forbindelse med beskyttelsen af it-systemer og data, så længe det potentielle afkast vurderes at være betydeligt.

Vi forpligter os til at overholde relevante lovgivninger og god praksis inden for it-sikkerhed, men vi prioriterer også hurtig udvikling og implementering af digitale løsninger, selvom det kan medføre øget risiko.“

RAPPORTERINGSGRÆNSER FOR ENKELTHÆNDELSER

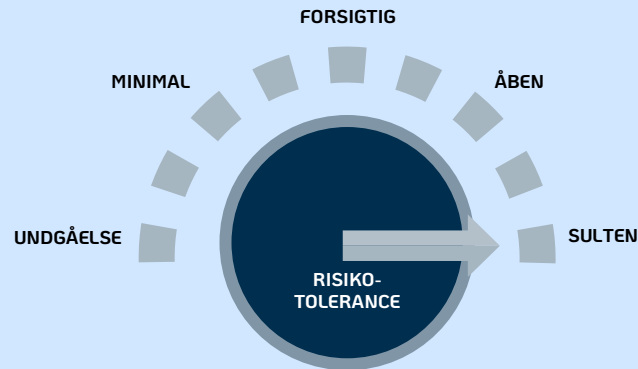
Bestyrelsen skal orienteres om hændelser via de almindelige rytmer for rapportering hvis tilgængeligheden til virksomhedens systemer er væsentligt forringet eller afbrudt i mere end 1 uge.

Bestyrelsen skal orienteres om hændelser via de almindelige rytmer for rapportering hvis følsomme oplysninger i virksomheden bliver (eller formodes at være) tilgået af ondsindede eksterne aktører eller hvis hændelsen formodes at kunne resultere i negativ medieopmærksomhed.

VILLIGHED TIL AT ABSORBERE TAB FRA IT-HÆNDELSER

Af tabellen til venstre fremgår risikotolerancen for hvert af de fem risikoområder. Tallene læses som en villighed til et årligt tab med en vis sandsynlighed.

NÅR RISIKOTOLERANCEN ER 'SULTEN'



Villighed til at absorbere tab

	Fysiske hændelser	Eksterne ondsindede angreb (cyber)	Interne ondsindede angreb	Interne fejl og mangler	Hændelser fra outsourcing
5%	1.000.000	10.000.000	1.000.000	1.000.000	1.000.000
50%	500.000	5.000.000	500.000	500.000	500.000
95%	250.000	1.000.000	250.000	250.000	250.000

GENEREL BESKRIVELSE AF RISIKOTOLERANCEN

Vi ønsker at tage betydelige risici for at fremme innovation og udvikling.

Vi er villige til at acceptere høj risiko for it-systemer og data.

Vi er parate til at eksperimentere med nye teknologier og løsninger, selvom de indebærer en betydelig usikkerhed.

RAPPORTERINGSGRÆNSER FOR ENKELTHÆNDELSER

Bestyrelsen skal orienteres om hændelser via de almindelige rytmer for rapportering hvis følsomme oplysninger i virksomheden bliver (eller formodes at være) tilgået af ondsindede eksterne aktører eller hvis hændelsen formodes at kunne resultere i væsentlig negativ medieopmærksomhed.

VILLIGHED TIL AT ABSORBERE TAB FRA IT-HÆNDELSER

Af tabellen til venstre fremgår risikotolerancen for hvert af de fem risikoområder. Tallene læses som en villighed til et årligt tab med en vis sandsynlighed