KØBSTÆDERNES FORSIKRING

Sammenligningsskema – oversigt over væsentlige vilkårsændringer.

Vilkår TE-CyberBasis-01 ændres til TE-CyberBasis-02

I skemaet kan du se de væsentligste vilkårsændringer for din CyberBasis forsikring.

Husk at du kan slå op i vilkårsdokumentet for at se forsikringernes fulde dækninger. Både de gamle og nye vilkår finder du på vores hjemmeside.

Generelle vilkår

Forbedring Præcisering Skærpelse

	Gamle vilkår	Nye vilkår
Status	TE-CyberBasis-01	TE-CyberBasis-02
+	**pkt. 1.1.c** ikke tidligere tilbudt	**pkt. 1.1.c** Forsikringen dækker rimelige og nødvendige omkostninger til at en ekspert kommer med rimelige anbefalinger om, hvordan, du kan styrke dit computersytems modstandskraft mod lignende fremtidige cyberhændelser.
!	**pkt. 1.1.f** for udgifter til juridisk forsvar, i forbindelse med en sag, anlagt af tilsynsmyndighederne mod dig.	**pkt. 1.1.f** for juridiske omkostninger, der er afholdt for at reagere på handlinger truffet af tilsynsmyndighederne med hensyn til Cyberhændelsen.
!	**pkt. 1.2** Forsikringen dækker rimelige og nødvendige omkostninger, som du har pådraget dig, for at retablere og konfigurere dine data, din software og dit computersystem efter en cyberhændelse, så tæt som muligt til den tilstand, som de var i umiddelbart forud for cyberhændelsen.	**"pkt. 1.2.a** Forsikringen dækker rimelige og nødvendige omkostninger, som du har pådraget dig som følge af en faktisk eller formodet cyberhændelse, a. for at retablere og konfigurere dine data, din software og dit computersystem efter en cyberhændelse, så tæt som muligt til den tilstand, som de var i umiddelbart forud for cyberhændelsen. Dette omfatter ikke omkostninger til forskning og re-udvikling af data og/eller software, som ikke kan gendannes."
+	**pkt. 1.2.b** Ikke tidligere tilbudt	**"pkt. 1.2.b** Forsikringen dækker rimelige og nødvendige omkostninger, som du har pådraget dig som følge af en faktisk eller formodet cyberhændelse, b. for at udskifte din hardware, hvis en ekspert har fastslået, at udskiftningen af din hardware (eller en del heraf) vil være mere effektiv og økonomisk end at dekontaminere (rense) eller omkonfigurere dit computersystem. Denne dækning omfatter ikke omkostninger til udskiftning af hardware indeholdt i Operationel Teknologi (OT) og indlejrede systemer. Den udskiftede hardware skal være af tilsvarende standard og funktionalitet som din eksisterende hardware før cyberhændelsen."

!	**"pkt. 2.1.5** Forsikringen dækker ikke et krav fra dig i henhold til denne forsikring, som udspringer direkte eller indirekte af følgende: Krig, herunder handlinger fra udenlandske fjenders side, fjendtligheder eller krigslignende aktiviteter (uanset om krig er erklæret eller ej), borgerkrig, invasion, opstand, oprør, revolution eller militærkup, herunder handlinger der foretages af en statslig myndighed for at hindre eller forsvare sig mod nogle af disse,"	**pkt. 2.1.5** Forsikringen dækker ikke et krav fra dig i henhold til denne forsikring, som udspringer direkte eller indirekte af følgende: Krig og/eller Statsstøttede cyberangreb,
−	**2.1.9** Forsikringen dækker ikke et krav fra dig i henhold til denne forsikring, som udspringer direkte eller indirekte af følgende: Din forsætlige, ondsindede eller bevidste handling eller undladelse,	**2.1.9** Forsikringen dækker ikke et krav fra dig i henhold til denne forsikring, som udspringer direkte eller indirekte af følgende: Din eller din serviceudbyders forsætlige, ondsindede eller bevidste handling eller undladelse,
!	**"pkt. 2.1.19** Tredjemandskrav fremsat af eller på vegne af: en juridisk enhed med reel kontrol over dig, nogle af dine datterselskaber, en juridisk enhed, som du eller dine datterselskaber har reel kontrol, en person som ejer en majoritetsaktiepost over dig, en juridisk enhed, som du har en økonomisk interesse i uanset beløbets størrelse, eller et partnerskab eller joint venture, som du er part i,"	**pkt. 2.1.19** Tredjemandskrav fremsat af eller på vegne af: en juridisk enhed med reel kontrol over dig, nogle af dine datterselskaber, en juridisk enhed, som du, dit moderselskab, eller dine datterselskaber har reel kontrol, en person som ejer en majoritetsaktiepost over dig, en juridisk enhed, som du har en økonomisk interesse i uanset beløbets størrelse, eller et partnerskab eller joint venture, som du er part i,
!	**pkt. 2.1.23** Omkostninger til forbedring af dit computersystem ud over den tilstand, det var i forud for forsikringsbegivenheden, medmindre det er uundgåeligt i forbindelse med gendannelse af data eller software eller aktiviteter forbundet med håndtering af IT-sikkerhedshændelser, som er dækket af denne forsikring.	**pkt. 2.1.23** Omkostninger til forbedring af dit computersystem eller dine data ud over den tilstand, det var i forud for forsikringsbegivenheden, medmindre det er uundgåeligt i forbindelse med gendannelse af data eller software eller aktiviteter forbundet med håndtering af IT-sikkerhedshændelser, som er dækket af denne forsikring.
−	**pkt. 2.1.25** Ikke tidligere undtaget	**pkt. 2.1.25** Tab af eller beskadigelse af digitale gavekort, tilgodebeviser eller anden digital- eller virtuel valuta.
+	**pkt. 4.3.1** tidligere opkrævet selvrisiko.	**pkt. 4.3.1** Selvrisiko opkræves ikke for omkostninger, som du har pådraget dig som følge af en faktisk eller formodet cyberhændelse omfattet af vilkårenes pkt. 1.1 a-e indenfor de første 48 timer.
!	**"pkt. 6.2.c** Det er en betingelse for forsikringsdækningen at Du: c. beskytter dine computersystemer og computernetværk mod cyberhændelser ved tilstrækkelige og regelmæssigt opdaterede - kodeord, - systemkonfigurationer, - firewalls"	**"pkt. 6.2.c** Det er en betingelse for forsikringsdækningen at Du: c. beskytter dine computersystemer og computernetværk mod cyberhændelser ved tilstrækkelige og regelmæssigt opdaterede - Stærk adgangskode, - systemkonfigurationer og - firewalls"

	"pkt. 6.2.c Det er en betingelse for forsikringsdækningen at Du: c. beskytter dine computersystemer og computernetværk mod cyberhændelser ved tilstrækkelige og regelmæssigt opdaterede - software-patches"	**"pkt. 6.2.d** Det er en betingelse for forsikringsdækningen at Du: d. installere og dokumentere sikkerhedsopdateringer (software patch) for al software og/eller firmware, inden for følgende tidsgrænser efter sikkerhedsopdateringen er blevet gjort tilgængelig: - Internetvendte computersystemer: 30 dage, - driftsteknologi (OT) og indlejrede systemer: 90 dage eller i henhold til anbefalinger fra den respektive fabrikant, - alle andre computersystemer: 60 dage. d. opgraderer, erstatter eller ophører med brugen af software eller hardware, som ikke længere understøttes af producenten, inden for en periode på tre måneder."
	pkt. 6.2.d opgraderer, erstatter eller ophører med brugen af software eller hardware, som ikke længere understøttes af producenten, inden for en periode på tre måneder.	**"pkt. 6.2.e** opgraderer, erstatter eller ophører med brugen af software eller hardware, som ikke længere understøttes af producenten, inden for en periode på tre måneder. I tilfælde af at sikkerhedsforholdsreglerne i punkt 6.2 (a) til (e) er outsourcet til en softwareproducent eller serviceudbyder, skal den eller de respektive serviceaftaler omfatte sammenlignelige kontraktlige forpligtelser, der skal opfyldes af softwareproducenten eller serviceudbyderen."
	"pkt. 6.2 Hvis du ikke overholder disse sikkerhedsforholdsregler, har forsikringsselskabet retten til at afvise betaling til dig i tilfælde af en cyberhændelse. Dog vil forsikringsselskabet ikke afvise betalingen til dig, hvis du beviser, at den manglende overholdelse af de ovennævnte sikkerhedsforholdsregler hverken var forsætlig eller groft uagtsom. Ligeledes vil forsikringsselskabet ikke afvise betalingen til dig, hvis du beviser, at cyberhændelsen ikke var forårsaget af eller blev forværret af den manglende overholdelse af de ovenstående sikkerhedsforholdsregler."	**"pkt. 6.2** Hvis du ikke overholder disse sikkerhedsforholdsregler, har forsikringsselskabet retten til at afvise betaling til dig i tilfælde af en cyberhændelse. Dette gælder dog ikke for omkostninger i henhold til punkt. 1.1 (a) til (e), indtil den manglende overholdelse af sikkerhedsforholdsreglerne er blevet konstateret af forsikringsselskabet eller en ekspert. Dog vil forsikringsselskabet ikke afvise betalingen til dig, hvis du beviser, at den manglende overholdelse af de ovennævnte sikkerhedsforholdsregler hverken var forsætlig eller groft uagtsom. Ligeledes vil forsikringsselskabet ikke afvise betalingen til dig, hvis du beviser, at cyberhændelsen ikke var forårsaget af eller blev forværret af den manglende overholdelse af de ovenstående sikkerhedsforholdsregler."
	ikke tidligere krævet	**"pkt. 7.2.b** Du skal stille optegnelser og dokumentation til rådighed for forsikringsselskabet vedrørende overholdelse af sikkerhedsforholdsreglerne i punkt 6.2 efter at en cyberhændelse er blevet rapporteret til forsikringsselskabet."

⛔	ikke tidligere krævet	**pkt. 7.2.c** Du skal stille tekniske rapporter til rådighed for forsikringsselskabet, når disse er afsluttet. De tekniske rapporter skal omfatte professionelle tekniske erklæringer vedrørende: indledende adgang (inkl. relevante udnyttelser og sårbarheder), yderligere bevægelser i forbindelse med cyberangrebet og dine aktiviteter angående software-patching.
❗	ikke tidligere præciseret	**pkt. 8.2 Back-up** Sikkerhedskopiering af dine data, som er egnet til at gendanne dine originale data til den sidste fungerende konfiguration før indtræden af forsikringsbegivenheden. Sikkerhedskopier skal opbevares på et lagringsmedie eller et computersystem, som er afbrudt fra det computersystem, der indeholder de originale data, for at sikre, at dine originale data og sikkerhedskopier ikke samtidig kan blive påvirket af en forsikringsbegivenhed. Egnede backup løsninger kan for eksempel være: lokale backups, netværks backups eller cloud backups.
❗	**"pkt. 8.6 Cyberhændelse** En ondsindet handling (herunder et DoS-angreb eller tyveri af data), malware, en menneskelig fejl, som har indvirkning på dine computersystemer eller en Serviceudbyders computersystemer eller en rimelig mistanke om samme."	**"pkt. 8.7 Cyberhændelse** En ondsindet handling (herunder et DoS-angreb eller tyveri af data), malware, en menneskelig fejl, som har indvirkning på dine computersystemer eller en Serviceudbyders computersystemer."
❗	**"pkt. 8.7 Cyberterrorisme** En handling udført af en enkeltperson eller gruppe af enkeltpersoner via brugen af computersystemer, for at skade, ødelægge, forstyrre eller tilgå dine computersystemer eller computernetværk, med religiøse, ideologiske eller politiske formål, herunder, men ikke begrænset til indflydelse på en regering og/eller for at indgyde frygt i offentligheden eller en del af offentligheden."	**"pkt. 8.8 Cyberterrorisme** En handling udført af en enkeltperson eller gruppe af enkeltpersoner via brugen af computersystemer, for at skade, ødelægge, forstyrre eller tilgå dine computersystemer eller computernetværk, med religiøse, ideologiske eller politiske formål, herunder, men ikke begrænset til indflydelse på en regering og/eller for at indgyde frygt i offentligheden eller en del af offentligheden. Dette inkluderer ikke statstøttede cyberangreb, som altid forbliver undtaget."
❗	Ikke tidligere præciseret	**"pkt. 8.22 ICS** Omfatter forskellige kontrolsystemer og tilhørende instrumentering (hardware og/eller software), der anvendes til industriel processtyring."
❗	Ikke tidligere præciseret	**"pkt. 8.23 Indlejrede systemer** Et computersystem, der har en dedikeret funktion og er indlejret i et større mekanisk eller elektronisk system."
❗	**pkt. 2.1.5** Krig, herunder handlinger fra udenlandske fjenders side, fjendtligheder eller krigslignende aktiviteter (uanset om krig er erklæret eller ej), borgerkrig, invasion, opstand, oprør, revolution eller militærkup, herunder handlinger der foretages af en statslig myndighed for at hindre eller forsvare sig mod nogle af disse,	**"pkt. 8.31 Krig** Væbnet konflikt, der involverer fysisk magt: - af én suveræn stat mod en anden suveræn stat, eller - som led i en borgerkrig, oprør, revolution, opstand, militær handling eller magtovertagelse, Uanset om der er erklæret krig eller ej."

	Ikke tidligere præciseret	**"pkt. 8.37 Operationel Teknologi (OT)** En samling af hardware og software, der kan påvirke en sikker, og pålidelig drift af en industriel proces. OT-miljøer overvåger normalt fysiske processer indenfor fremstilling, energi, medicin, bygningsforvaltning og økosystemer inden for andre industrier. OT inkluderer, men er ikke begrænset til, ICS og SCADA."
	ikke tidligere præciseret	**"pkt. 8.43 SCADA (Supervisory Control and Data Acquisition)** En samling af kontrolsystemer (hardware og/eller software), som indsamler data i realtid fra aktiver i industrielle miljøer, for at kontrollere udstyret og dets forhold."
	ikke tidligere præciseret	**"pkt. 8.46 Sikkerhedsopdateringer** Ændringer til en software, firmware eller dens understøttende data, designet til at opdatere, rette eller forbedre den. Dette inkluderer rettelser til sikkerhedssårbarheder og andre fejl, der typisk leveres af softwareleverandører til operativsystem- og applikationsopdateringer for at forbedre sikkerheden, funktionaliteten, brugervenligheden eller ydeevnen af et program i tide."
	ikke tidligere præciseret	**"pkt. 8.48 Statsstøttet cyberangreb** Brug af et computersystem, under ledelse af eller under kontrol af en suveræn stat til at forstyrre, nægte adgang til eller forringe funktionaliteten af et omputersystem og/eller kopiere, fjerne, manipulere, nægte adgang til eller ødelægge information i et computersystem. På trods af forsikringsselskabets bevisbyrde, som forbliver uændret, vil du og forsikringsselskabet overveje alle tilgængelige, objektive og rimelige beviser, for at tilskrive et Statsstøttet cyberangreb til en suveræn stat. Dette kan omfatte formel eller officiel tilskrivning fra regeringen af den stat, hvor computersystemerne, der er berørt af et Statsstøttet cyberangreb fysisk er placeret, til en anden suveræn stat eller dem, der handler efter dens ledelse eller under dens kontrol."
	ikke tidligere præciseret	**"pkt. 8.49 Stærk adgangskode** Adgangskode bestående af 8 eller flere tegn, i en kombination af mindst tre af følgende: - store bogstaver - små bogstaver - specielle symboler - tal Brugen af gentagne tegn (f.eks. ""1234"", ""1111"", ""abcde""), tastaturmønstre (f.eks. ""asdfgh"") eller brugen af personlige oplysninger om medarbejderen (f.eks. fødselsdatoer, vejnavne) skal undgås."