Cyberforsikring
Forsikringsbetingelser nr. CY2512

Aftalegrundlag

Forsikringen består af forsikringsaftalen (policen), eventuelle tillæg og forsikringsbetingelserne.
For forsikringen gælder endvidere Lov om Forsikringsaftaler og Lov om forsikringsvirksomhed i det omfang, disse ikke er fraveget.

Tilsyn og Garantifond

Tryg er underlagt tilsyn af Finanstilsynet og er tilsluttet Garantifonden for skadeforsikringsselskaber.

Behandling af personoplysninger og samtykke

På www.tryg.dk/personoplysninger findes yderligere om, hvordan Tryg behandler følsomme oplysninger.
Her beskrives, hvor oplysningerne bliver registreret, og hvem oplysningerne eventuelt bliver videregivet til. Tryg kan altid kontaktes, såfremt sikrede ønsker at vide mere.

Yderligere oplysninger

Yderligere oplysninger om forsikringsdækningen findes på www.tryg.dk.

Tryg | Klausdalsbrovej 601 | 2750 Ballerup
70 11 20 20 | www.tryg.dk
Tryg Forsikring A/S | CVR-nr. 24260666

Når sikrede læser betingelserne

- Forsikringsaftalen viser de dækninger, summer og selvrisikobeløb, som sikrede har valgt for forsikringen.
- For at sikre at en skade er dækket, skal sikrede se under både den konkrete forsikringsdækning og under de generelle bestemmelser.
- Vær opmærksom på, hvordan erstatningen beregnes.

Hvis der sker en skade

- Sikrede skal straks anmelde skaden til Tryg på telefon 44 20 61 40.
- Sikrede skal indgive en politianmeldelse, ved enhver anmeldt skade på forsikringen.
- Sikrede er forpligtet til at følge den vejledning og anvisning, som sikrede modtager af Tryg og Trygs samarbejdspartnere, herunder medvirke til at indgå databehandler*-aftaler med Trygs samarbejdspartnere, således at skade og tab kan minimeres mest muligt. I modsat fald kan det få betydning for, i hvilket omfang skaden er dækket, og erstatning kan blive nedsat eller helt bortfalde.

Indholdsfortegnelse

		Side
1.	**Hvad skal sikrede selv sørge for**	3
1.1	Hvis der sker ændinger	3
1.2	Retten til erstatning	3
2.	**Hvem er omfattet**	3
2.1	Sikrede	3
3.	**Hvor gælder forsikringen**	3
3.1	Geografisk dækningsområde	3
4.	**Hvornår gælder forsikringen**	3
4.1	Konstateret tab	3
4.2	Flere skader/tab, der skyldes samme årsag	4
4.3	Efteranmeldelse	4
4.4	Forsikringssum	4
5.	**Hvad dækker forsikringen**	4
5.1	Cyber	4
5.2	Cyber Driftstab	4
5.3	Datatab	5
5.4	Datatab - Ansvar	5
5.5	ID-Tyveri	6
5.6	Cybersvindel	6
5.7	Cybersikker	6
6.	**Generelle undtagelser**	7
7.	**Hvis skaden sker**	8
7.1	Skadebehandling	8
7.2	Krav mod tredjemand	8
8.	**Generelle bestemmelser**	9
8.1	Forsikring i andet selskab	9
8.2	Forsikringens varighed	9
8.3	Forsikringens betaling	9
8.4	Gebyrer	9
8.5	Indeksregulering	10
8.6	Præmieregulering og ændring af forsikringsbetingelser	10
8.7	Ansvarlige forretningsprincipper	10
9.	**Moms**	10
10.	**Lovvalg og værneting**	10
11.	**Ordforklaring**	11

1. Hvad skal sikrede selv sørge for

1.1 Hvis der sker ændringer

Tryg beregner forsikringens pris på baggrund af de oplysninger, der fremgår af forsikringsaftalen. Sker der ændringer, skal Tryg have besked. Hvis forsikringens oplysninger ikke længere er rigtige, kan det få den konsekvens, at sikredes ret til erstatning efter en skade eller tab bliver nedsat eller helt bortfalder.

1.2. Retten til erstatning

Retten til erstatning er betinget af, at sikrede:

- Anvender en opdateret EDR-software* eller antivirus på alle klienter og servere - samt IoT-enheder* og mobile enheder. Sikrede er forpligtet til straks at reagere på alarmer og advarsler fra den anvendte EDR-software* eller antivirus, for at minimere risikoen for skader.
- Tager en fuld backup* af samtlige forretningskritiske* data minimum hver 5. dag. Sikredes fulde backup* skal være sikrede i hænde, være fungerende og læsbar, indenfor 72 timer fra forsikringsbegivenheden er indtrådt.
- Hvor der tages backup* på lokale medier, opbevarer data* i særskilt aflåst bygning eller aflåst databrand- eller sikkerhedsskab.
- Beskytter computere og netværk med en stærk adgangskode* bestående af mindst 14 tegn, der skiftes mindst hver 12. måned. Adgangskoden* skal bestå af mindst en kombination af store og små bogstaver og tal.
- Hvor der tages backup via en online udbyder, sikrer at forbindelsen mellem sikrede og udbyder krypteres.
- Ved enhver tilslutning til backup anvender MFA*, uanset om der er tale om intern eller ekstern tilslutning.
- Anvender MFA* på alle enheder, ved enhver ekstern tilslutning til sikredes netværk, systemer, servere, og lignende. Gælder både interne og eksterne brugere.
- Ved enhver tilslutning til sikredes Sociale Medier businesskonto, på henholdsvis Facebook og Instagram, anvender MFA*, uanset om der er tale om intern eller ekstern tilslutning. Privat Facebook- og Instagramkonto er ikke omfattet af forsikringen.
- Ved adgang til eksternt hostede forretningskritiske systemer, anvender MFA*.
- Beskytter mobile enheder og tablets med adgangs- eller pin-kode*.
- Ikke anvender default adgangskode* eller default bruger-id på sikredes systemer.
- Fysisk har sikret adgangen til netværk og IT-udstyr mod uvedkommende adgang.
- Der er en del af et kontorfællesskab med delt internet, har eget adskilt netværk med egen opdateret EDR-software* eller antivirus, eller anvender VLAN segmenteret netværk, der isolerer sikredes systemer.
- Ikke deler printernetværk med andre virksomheder, eller tredjemand.
- Kun anvender operativsystemer/styresystemer, der er understøttet og supporteret af producenten med løbende sikkerhedsopdateringer.
- Sørger for kontinuerlig opdatering af internetprogrammer, herunder 3. parts programmer (fx Java, Adobe Reader og internet browsere) til seneste version.

Hvis en eller flere af ovennævnte sikkerhedsforholdsregler ikke er overholdt, kan erstatningen bortfalde jf. Forsikringsaftaleloven.

2. Hvem er omfattet

2.1 Sikrede

Sikrede er den eller de virksomheder der fremgår af policen, og som har ret til erstatning eller beskyttelse ved en dækningsberettiget skade.

Forsikringen dækker den eller de danske virksomheder, der er angivet på policen, men omfatter ikke virksomheder i Grønland eller på Færøerne. Datterselskaber og filialer er kun omfattet, hvis de specifikt er nævnt på policen.

Forsikringen kan udvides til at omfatte datterselskaber og filialer i Skandinavien.

3. Hvor gælder forsikringen

3.1 Geografisk dækningsområde

Forsikringen dækker i Danmark, dog også datterselskaber og filialer i Skandinavien, der specifikt er nævnt på policen. Samt under rejser og midlertidigt ophold i Europa, uanset hvor angrebet finder sted.

4. Hvornår gælder forsikringen

4.1 Konstateret tab

Forsikringen dækker tab der konstateres af sikrede i forsikringstiden, samt tab der relaterer sig til omstændigheder, der konstateres i forsikringstiden.

Forsikringen dækker ikke forsikringsbegivenheder der er indtrådt før forsikringens ikrafttræden.

4.2 Flere skader/tab, der skyldes samme årsag

Flere skader eller tab, der har den samme årsag, betragtes som én samlet skade eller ét samlet tab.

4.3 Efteranmeldelse

Tab der konstateres i forsikringstiden, men som anmeldes mere end 3 måneder efter forsikringens ophør, er ikke dækket af forsikringen.

4.4 Forsikringssum

Den samlede forsikringssum på policen, beregnet som summen af de individuelle dækninger, kan maksimalt udgøre 10 millioner kr. pr. forsikringsår, beregnet ud fra policens årlige hovedforfaldsdato.

De valgte forsikringssummer fremgår af policen.

5. Hvad dækker forsikringen

Det fremgår af forsikringsaftalen, hvilke dækninger, summer og selvrisikobeløb, sikrede har valgt for forsikringen

5.1 Cyber

(gælder kun, hvis det fremgår af forsikringsaftalen)

Forsikringen dækker nødvendige, rimelige og dokumenterede omkostninger til rekonstruktion af sikredes IT-systemer, netværk, software og forretningskritiske* data* som krypteres, slettes, fjernes eller beskadiges som følge af et direkte, ondsindet angreb af skadelig karakter fx

- Virus*
- Ransomware*
- Hacking
- DDoS-angreb*
- Website hijacking*
- Website defacement*

Endvidere dækker forsikringen rimelige, nødvendige og dokumenterede omkostninger til rekonstruktion af sikredes software og data* som følge af

- Systemnedbrud efter opsætning eller opdatering af programmer og systemsoftware. Dog dækkes ikke nedbrud, der udelukkende vedrører trådløst netværk (Wi-Fi), internetforbindelse eller interne netværk.
- Handlinger begået af ansatte med det formål at skade sikredes data*.

Data* som sikrede har lagret på eksterne servere, herunder via cloud-, SaaS- eller hostingløsninger hos serviceudbydere, betragtes som sikredes data*.

Sikredes data* og software er omfattet af forsikringen, uanset hvor i verden disse er lagret eller hostet.

Forsikringen dækker omkostninger, der afholdes i op til 6 måneder efter, at sikrede har konstateret en dækningsberettiget skade eller et dækningsberettiget tab.

5.2 Cyber Driftstab

(gælder kun, hvis det fremgår af forsikringsaftalen)

5.2.1 Hvilke tab erstattes

Forsikringen dækker – uanset forsikringsbetingelsernes "Generelle undtagelser" - sikredes dokumenterede driftstab, der skyldes nedgang i omsætningen af varer og tjenesteydelser som følge af en forsikringsbegivenhed, der er dækket under Cyber-dækningen afsnit 5.1.

5.2.2 Hvilke tab erstattes ikke

Ud over de under punktet "Generelle undtagelser" nævnte undtagelser, dækker forsikringen ikke omkostninger, tab, driftstab eller forøgelse af driftstab, der skyldes

- Strejke eller lockout.
- Forsinkelse af sikredes genoptagelse som følge af kapitalmangel, forbedringer eller udvidelser.
- Computerstyret produktionsudstyr, bearbejdningsmaskiner eller andet automatiseret eller digitalt styret udstyr, der helt eller delvist mister funktionalitet som følge af skade.

5.2.3 Dækningsperiode
Dækningsperioden starter på det tidspunkt, hvor en dækningsberettiget skade konstateres og ophører det antal måneder senere, som fremgår af forsikringsaftalen og på samme tidspunkt af døgnet som starttidspunktet.

5.2.4 Karenstid
Forsikringen dækker ikke driftstab i karenstiden.
Karenstiden fremgår af forsikringsaftalen og starter på det tidspunkt, hvor en dækningsberettiget skade konstateres.

5.2.5 Sikredes forpligtelser
Det er en betingelse for dækning, at sikrede - udover bestemmelserne i afsnit 8.9 - skal forsøge at opretholde omsætning af varer og tjenesteydelser. Tryg dækker efter aftale rimelige omkostninger hertil. Omkostningerne kan ikke overstige det driftstab, der ellers ville opstå, og erstattes kun, hvis de afholdes inden for dækningsperioden.

Sikrede er forpligtet til at samarbejde med Tryg med henblik på at afværge eller begrænse driftstabet.

5.2.6 Opgørelse af driftstabet
Driftstabet opgøres som forskellen mellem
- den forventede omsætning med fradrag af det forventede forbrug af indkøbte handelsvarer til videresalg samt råvarer, halvfabrikata og produktrelateret emballage, og
- den konstaterede omsætning med fradrag af det konstaterede forbrug af indkøbte handelsvarer til videresalg samt af råvarer, halvfabrikata og produktrelateret emballage.

Fra dette beløb trækkes sparede omkostninger, herunder lønomkostninger, som sikrede kan frigøre sig for. Dog ikke lærlinge- og funktionærlønninger.

Derudover dækkes rimelige meromkostninger. Meromkostningernes størrelse og art aftales i hvert enkelt tilfælde med Tryg.
Ved omsætning forstås faktureret omsætning ekskl. merværdiafgift, ydede rabatter, bonus og anden salgsreduktion.

Sikrede har ret til at producere til lager i det omfang, afsætningsmæssige forhold kræver dette. Salgsværdien af det lager, der er blevet opbygget i dækningsperioden, og som ligger ud over denne berettigede lageropbygning, trækkes fra den omsætningsnedgang, der udregnes.

5.2.7 Revisor-omkostninger
Inden for forsikringssummen dækkes rimelige omkostninger til sikredes sædvanligt anvendte revisor i forbindelse med opgørelsen af et erstatningsberettiget driftstab.

Disse omkostninger dækkes med indtil 15% af erstatningen for selve driftstabet, dog højest 179.361 kr., indeksreguleret (2025).

Omkostningernes størrelse aftales på forhånd i hvert enkelt tilfælde med Tryg.

5.2.8 Nedlukning af sikrede
Hvis sikrede ikke genoptages efter en konstateret forsikringsbegivenhed, bliver driftstabet udregnet for det tidsrum (inden for dækningsperioden), der normalt ville gå, før sikrede kunne være i drift.

Der erstattes kun den del af driftstabet, der svarer til uundgåelige, forsikrede omkostninger, som bevisligt er afholdt. Dette gælder dog ikke, hvis sikrede ikke bliver genoptaget på grund af forhold, som sikrede ikke er herre over.

5.3 Datatab
(gælder kun, hvis det fremgår af forsikringsaftalen)

5.3.1 Forsikringen dækker
Ved mistanke om eller konstatering af utilsigtet videregivelse af tredjemands personoplysninger* dækker forsikringen nødvendige, rimelige og dokumenterede omkostninger til
- information og rådgivning om gældende regler, herunder rådgivning om, hvorledes situationen håndteres
- vurdering af behov for og ydelse af eksperthjælp til afdækning af, hvorvidt mistanke er begrundet eller der er sket et brud
- vurdering af indberetnings- og underretningspligt over for myndighed i henhold til gældende lovgivning og berørte parter (de registrerede)
- indberetning og underretning, jf. punktet ovenfor.

5.3.2 Forudsætninger for dækning
Det er en forudsætning for dækning, at årsagen til videregivelse af tredjemands personoplysninger* er utilsigtet, og ikke skyldes sikredes medarbejderes, eller egne forsætlige handlinger, eller grove uagtsomhed.

Det er endvidere en forudsætning, at sikrede – ved brug af databehandler* - benytter skriftlige aftaler, således at begge parter er bekendt med de krav, som loven stiller vedrørende behandling af personoplysninger*, jf. den til enhver tid gældende lovgivning.

5.4 Datatab - Ansvar
(overfor tredjemand gælder kun, hvis det fremgår af forsikringsaftalen)

5.4.1 Forsikringen dækker
Forsikringen dækker skadeserstatning, herunder godtgørelse for tort*, til tredjemand. Det er en forudsætning, at kravet er en følge af sikredes utilsigtede videregivelse af personoplysninger*, eller oplysninger tilhørende tredjemand, som sikrede juridisk er forpligtet til at holde fortrolige, når videregivelse medfører overtrædelse af lovgivning om behandling og opbevaring af personoplysninger.

Det forudsættes at:
- oplysningerne er indhentet og registreret i overenstemmelse med gældende lovgivning
- videregivelsen sker fra sikredes netværk* samt at videregivelsen har påført tredjemand dokumenteret skade eller tab, som sikrede er erstatningsansvarlig for. Eller at tredjemand har været udsat for en krænkelse, for hvilken sikrede er pligtig til at betale godtgørelse for tort
- videregivelsen ikke skyldes handlinger udført forsætligt eller groft uagtsomt af dig eller sikredes ansatte.

Forsikringen dækker endvidere rimelige, nødvendige og dokumenterede omkostninger til afdækning af, hvorvidt der foreligger en dækningsberettiget forsikringsbegivenhed.

Forsikringen dækker kun hvis omkostningerne er accepteret af Tryg.

5.4.2 Udgifter til genetablering af renommé
Forsikringen dækker endvidere sikredes udgifter til public relation bureau og lignende til genetablering af sikredes eget renommé.

Det forudsættes at:
- renommé-tabet er afledt af en dækningsberettiget skade, jf. punkt 5.4.1
- sikredes rolle i sagen har været negativt omtalt i landsdækkende medier
- omtalen har haft væsentlig negativ indflydelse på sikredes renommé.

Ved genetablering af sikredes eget renommé gælder der en tidsmæssig dækningsperiode på 18 måneder fra den dækningsberettigede skade, der forårsagede behovet for udgift til genetablering af sikredes eget renommé.

Dækningssummen udgør maksimalt 100.000 kr.

5.4.3 Særlige undtagelser
Udover de undtagelser, der er nævnt i afsnit 6. Generelle undtagelser, dækker forsikringen ikke tab eller skade, der stammer fra oplysninger om kredit- og debetkort.

5.4.4 Geografisk afgrænsning
Uanset punkt 3.1 dækker forsikringen alene erstatningsansvar for skade eller tab indtruffet indenfor EU, medmindre andet fremgår af forsikringsaftalen.

5.5 ID-Tyveri*
(gælder kun, hvis det fremgår af forsikringsaftalen)

5.5.1 Forsikringen dækker
Forsikringen dækker følgende assistance til forebyggelse, opdagelse eller begrænsning af de økonomiske skadevirkninger efter tredjemands tyveri og/eller misbrug af sikredes identitet:
- Ved angreb på sikredes Sociale Medie business-konto, hvor sikredes data på Facebook eller Instagram kompromitteres og anvendes uden sikredes tilladelse, vil Trygs udpegede it-eksperter yde juridisk og teknisk assistance for at genetablere kontrollen over kontoen. Dette forudsætter, at adgangen kan etableres.
- Opdagelse af mulig økonomisk svindel og kortlæggelse af omfanget.
- Rådgivning og information om sikredes juridiske og økonomiske situation.
- Nødvendige indsatser for at begrænse økonomiske tab, forebygge yderligere økonomisk tab og afvise uretmæssige pengekrav.
- Vejledning omkring anmeldelse til Politiet.
- Hjælp til at genoprette sikredes kreditværdighed, kontakt til kreditorer mv.
- Hjælp til korrektion af fejloplysninger hos Erhvervsstyrelsen og andre relevante myndigheder eller parter.

Herudover dækkes direkte omkostninger til juridisk bistand hos et dansk advokatfirma, hvis det skønnes nødvendigt for at afvise uberettigede pengekrav eller en uberettiget registrering hos et kreditoplysningsbureau som fx RKI.

Dækningssummen for juridisk bistand udgør 30.589 kr. pr. skade eksklusiv moms, indeksreguleret (2025).

5.5.2 Sikredes forpligtelser
Så snart sikrede får formodning om eller kendskab til et tyveri eller misbrug af sikredes identitet skal sikrede uden ophold anmelde dette til Tryg.

Såfremt sikrede får formodning om eller kendskab til et kriminelt forhold skal sikrede tillige foretage anmeldelse til politiet.

5.6 Cybersvindel
(gælder kun, hvis det fremgår af forsikringsaftalen)

Cybersvindel refererer til alle former for digital eller teknisk manipulation, hvor svindleren (tredjemand) narrer medarbejdere eller virksomhedsejer til at overføre penge eller give adgang til systemer. Dette kan ske gennem phishing*, fakturasvindel*, BEC* eller social engineering*, hvor ofrene uforvarende bliver snydt via manipulerende henvendelser.

5.6.1 Forsikringen dækker
Forsikringen dækker sikredes dokumenterede økonomiske tab som følge af cybersvindel-angreb - samt når tabet skyldes et elektronisk indbrudstyveri* i sikredes netbank. Det er en betingelse for dækning at bankkontoen er tilknyttet sikredes CVR-nummer.

Forsikringen dækker op til den valgte forsikringssum på policen, og alene når det er sikrede der bliver udsat for cybersvindel eller elektronisk indbrudstyveri*.

Forsikringen for elektronisk indbrudstyveri dækker herudover:
- Trækningsret på sikredes bankkonto op til den aftalte grænse med banken.
- Kassekredit på sikredes bankkonto.
- Renter fra tidspunktet af tyveriet og indtil tyveriet opdages.
- Netbanksindbrud gennem tredjemands it-systemer.

Forsikringen dækker endvidere rimelige og nødvendige undersøgelsesomkostninger til at identificere omfanget af hændelsen. Dette inkluderer omkostninger til it-eksperter eller juridiske rådgivere udpeget af Tryg, og igangsættes kun med Trygs forudgående godkendelse. Undersøgelsesomkostninger ligger indenfor den valgte dækningssum på policen, og ikke i tillæg til summen.

5.6.2 Udbetaling af erstatning
Det er Tryg uvedkommende ved udbetaling af erstatning af sikredes økonomiske tab hvordan denne erstatning skattemæssigt skal behandles hos sikrede, og det er derfor sikrede selv, der skal afdække hvordan erstatningen skal behandles ved opgørelse af den skattepligtige indkomst. Tryg dækker ikke omkostninger ved eventuelle skattemæssige konsekvenser af erstatningen.

5.6.3 Hvilke tab erstattes ikke
Udover de undtagelser, der er nævnt i afsnit 6. Generelle undtagelser, dækker forsikringen ikke:
- Når sikrede, ejere eller medarbejdere har medvirket ved grov uagtsomhed eller forsæt, til aktiviteten eller hændelsen, der udløste forsikringsbegivenheden.
- Rekonstruktion af it-systemer, software og data, medmindre forsikringen er omfattet af afsnit 5.1. Cyber-dækningen. Det fremgår af policen om dækningen er omfattet af forsikringen.
- Når forsikringsbegivenheden skyldes brist i bankens sikkerhedsprocedurer.
- Tab, tyveri, værdiforringelse eller manglende adgang til kryptovaluta* – uanset årsag, herunder cyberangreb.
- Privatrelateret* svindel er ikke omfattet af forsikringen.

5.6.4 Geografisk dækningsområde
Forsikringen dækker uanset hvor i Verden den kriminelle handling er begået, men kun indestående på konti i danske pengeinstitutter samt deres danske datterselskaber og filialer i Europa. Det er en betingelse, at sikrede udelukkende benytter adgang gennem en dansk netbank.

5.6.5 Sikredes forpligtelser
Det er en forudsætning for dækning, at så snart sikrede får formodning om eller kendskab til omstændigheder der kan udløse en forsikringsbegivenhed, skal sikrede uden ophold anmelde dette til Tryg. Såfremt sikrede får formodning om eller kendskab til et kriminelt forhold, skal sikrede tillige foretage anmeldelse til Politiet.

Når en forsikringsbegivenhed er konstateret, skal sikrede forhindre yderligere skade, og begrænse tabet mest muligt ved vederlagsfrit at medvirke til at opklare sagen. Dette inkluderer at indsamle og levere bevismateriale og nødvendige oplysninger, som Tryg efterspørger.

Sikrede er også forpligtet til at lade Tryg, samt vores udpegede it-eksperter, foretage alle nødvendige undersøgelser for at fastslå, hvordan tabet er opstået og dets omfang – hvis Tryg vurderer det nødvendigt for behandling af skaden.

5.6.6 Betingelse for dækning
Det er en betingelse for dækning, udover bestemmelserne i afsnit 1.2 Retten til erstatning, at følgende sikkerhedsforholdsregler til enhver tid er overholdt:
- MFA* skal anvendes ved enhver tilslutning til netbank.
- Der skal logges af netbanken, når den ikke bruges.
- Computeren skal tastaturlåses, når den forlades.
- Sikrede skal straks efter en forsikringsbegivenhed er konstateret kontakte banken for at forsøge at tilbagekalde overførslen. Banken kan derefter tage de nødvendige skridt, såsom at kontakte den modtagende bank eller samarbejde med politiet og andre relevante myndigheder for at spore og inddrive pengene.
- Sikrede skal overholde de sikkerhedsregler, der er aftalt med pengeinstituttet med hensyn til elektroniske kontooverførsler, herunder overholder bankens til enhver tid forslåede sikkerhedsforanstaltninger.

Særligt vedr. fakturaer, vedhæftninger, links og oplysninger om pengeoverførsler:
- Ved modtagelse at e-mail der indeholder oplysninger omkring betaling, fx gennem links eller vedhæftninger, skal afsenderens identitet bekræftes, ved at sikrede kontrollerer og sikrer sig at afsenderens e-mailadresse matcher det officielle domænenavn* hvor mailen forventes af komme fra.
- Sikrede skal kontrollere og sikre at e-mailen kommer fra det forventede domæne*, samt at links fører til den forventede webside.
- At en sikker e-mail opsætning er etableret, så e-mails kan bekræftes at komme fra den rigtige afsender.
  Dette inkluderer opsætning af SPF*, DKIM* og DMARC*, der hjælper med at validere afsenderens identitet og beskytter mod uautoriseret forfalskning af e-mails.
- Ved betaling af fakturaer med beløb over 50.000 kr. skal betalingen altid valideres af mindst to godkendere. Den ansvarlige godkender skal sørge for at modtage en e-mailbekræftelse fra nærmeste chef eller revisor om, at fakturaen er korrekt og kan godkendes, før den endelige godkendelse finder sted. Når begge godkendere har valideret fakturaen, registreres den som godkendt og kan behandles til betaling.
- Ved intern anmodning om pengeoverførsler fra medarbejdere, direktører, bestyrelsesmedlemmer og lignende, med beløb over 50.000 kr., skal den ansvarlige godkender telefonisk bekræfte overførslen med anmoder. Efterfølgende skal en e-mailbekræftelse modtages fra alle involverede parter, før overførslen kan gennemføres.

Ovennævnte sikkerhedsforholdsregler gælder også for tredjemands IT-systemer, når sikrede har givet tredjemand fuldmagt til sikredes netbank.

5.6.7 Dokumentationskrav
Det er en betingelse for dækning, at sikrede beskriver hændelsen overfor Tryg, ved at fremlægge den nødvendige dokumentation.

Dette kan være en eller flere af nedenstående punkter:
- En detaljeret beskrivelse af, hvordan den kriminelle handling fandt sted, herunder hvornår og hvordan den blev opdaget, samt hvilke systemer eller data der blev påvirket.
- Tryg kan kræve fremlæggelse af systemlogfiler, sikkerhedsadvarsler, e-mails eller andre digitale fodspor, der viser angrebets omfang og karakter.
- Dokumentation af, at hændelsen er blevet rapporteret til bank og relevante myndigheder som f.eks. Politi eller Datatilsynet.
- En redegørelse for, hvad sikrede har gjort for at undersøge hændelsen internt. Dette kan inkludere interne revisionsrapporter, ændringer af systemer, eller sikkerhedsforanstaltninger, der er blevet implementeret efter hændelsen.
- Dokumentation for de økonomiske tab som følge af forsikringsbegivenheden.
- Hvis nødvendigt, kan forsikringsselskabet kræve erklæringer fra eksperter eller andre involverede parter, som kan bekræfte hændelsen og dens omfang.
- Kopier af breve, e-mails eller meddelelser, der er sendt til kunder, partnere, ansatte eller andre relevante personer, i forbindelse med hændelsen.

Det er vigtigt, at sikrede dokumenterer alle aspekter af hændelsen så præcist og detaljeret som muligt, da dette kan have betydning for, hvorvidt Tryg dækker tabet, og hvor hurtigt en erstatning kan udbetales.

5.7 Cybersikker

(gælder kun, hvis det fremgår af forsikringsaftalen)

Cybersikker er software, som efter installation på din sikredes enheder (PC'ere, mobiler og tablets), yder følgende typer af beskyttelse og anvendelse:

- Antivirusbeskyttelse
- Browserbeskyttelse med DNS-tjek
- Ransomwarebeskyttelse
- Bankbeskyttelse
- Administrationstjeneste
- Administration af firewall
- Privatslivs-VPN
- Adgangskodeboks (Password Manager)
- ID-overvågning

Brug af Cybersikker
Hver licens af Cybersikker giver adgang til installation af software på 25 af sikredes enheder. En enhed kan være en mobil, en tablet eller en PC. Hvis der er behov for installation af software på mere end 25 enheder, kan sikrede købe ekstra licenser hos Tryg.

Brug af Cybersikker for sikrede forudsætter, at it-udstyr og programmer understøtter og tillader installation af softwaren.

For at bruge Cybersikker skal sikrede installere softwaren. Dette sker ved, at sikrede videregiver sin e-mailadresse til Tryg i forbindelse med forsikringsaftalens indgåelse. Tryg videregiver e-mailadressen til den samarbejdspartner, der udbyder softwaren, som herefter via e-mail sender et aktiveringslink.

Brugsret og dataansvar
Under installation af softwaren på sikredes enheder skal samarbejdspartnerens generelle vilkår om brugsret og fortrolighedspolitik accepteres, før softwaren kan tages i anvendelse. Sikrede opnår med accept over for samarbejdspartneren en ikke-eksklusiv brugsret til sikkerhedsfunktionerne på de fastsatte licensvilkår.

Sikrede overtager ingen immaterielle rettigheder, ophavsrettigheder eller lignende ud over den tillagte brugsret. Samarbejdspartneren er selvstændigt dataansvarlig for de oplysninger, de indsamler og registrerer om sikrede. Sikrede skal tage kontakt til den samarbejdspartner, som Tryg har udpeget, hvis sikrede vil benytte retten til indsigt, gøre indsigelse mod behandlingen eller korrigere sikredes oplysninger hos den udpegede samarbejdspartner.

Videregivelse af nødvendige oplysninger
Tryg videregiver de nødvendige oplysninger om sikredetil den samarbejdspartner, som ejer softwaren, der skal installeres på sikredes enheder. Tryg videregiver første brugers e-mailadresse og fornavn, information om antal licenser samt et anonymiseret kundenummer for at samarbejdspartneren kan oprette, installere og servicere sikrede.

Samarbejdspartneren hjælper sikrede med installation, overvågning, løbende softwareopdatering, administration og support af softwaren på sikredes enheder.

Trygs ansvar
Sikrede har med de begrænsninger, der er anført nedenfor, ret til erstatning i henhold til dansk rets almindelige erstatningsregler for tab som følge af handlinger og undladelser forårsaget af os eller nogen, som Tryg har ansvaret for.

Sikrede gøres opmærksom på, at sikrede, til trods for installationen af Cybersikker, ved at færdes på internettet, ved at downloade materiale fra internettet, eller ved åbning af programmer modtaget pr. e-mail, løber en risiko for at kompromittere sikkerheden på det anvendte udstyr, og løber en risiko for at inficere din hardware og software med virus eller lignende. Tryg og Trygs samarbejdspartner har ikke indflydelse på disse forhold og kan således ikke drages til ansvar for skader og tab opstået som følge heraf, jf. pkt. 6. i Cyberforsikringens generelle undtagelsesbestemmelser.

Tryg er aldrig erstatningsansvarlige for indirekte tab, herunder tabt avance, produktionstab, tab som følge af tab af personlige data og installeret software og lignende, eller for tab som følge af uvedkommendes adgang til sikredes data og/eller systemer.

Det er alene sikredes ansvar, at sikredes it-udstyr og programmer understøtter og tillader installation af softwaren på sikredes egne og på medarbejdernes enheder.

Tryg er ikke ansvarlige for eventuelle driftsforstyrrelser i forbindelse med anvendelsen af Cybersikker.

6. Generelle undtagelser

6.1 Forsikringen dækker ikke skade, som er en direkte følge af

6.1.1 Krig og Cyberkrig

Forsikringen dækker ikke skader, tab, ansvar (herunder ansvar over for tredjemand), forsvarsomkostninger eller andre udgifter, der opstår som en direkte følge af krig, krigslignende handlinger, NBCR-terrorskader*, terrorisme*, neutralitetskrænkelse, borgerkrig, oprør, borgerlige uroligheder, cyberkrig*, cyberoperationer* eller cyberkrigsførelse*, herunder hybridkrig*.

Dette gælder også ved krig mellem stater, uanset om krigen er erklæret, i forberedelsesfasen eller i afslutningsfasen. Herunder statsstøttede angreb, udført med hjælp eller støtte fra en stat, der har til formål at beskadige, ødelægge eller på anden måde kompromittere sikredes systemer og data.

Dette inkluderer enhver form for destruktiv aktivitet rettet mod følgende digitale enheder og systemer, og uanset om én eller flere enheder eller systemer rammes:

- Computersystemer, Data, Software, Servere, Dataopbevaring, Netværksudstyr, Backup-data, Cloud opbevarede data, Mobile enheder, OT-enheder*, IoT-enheder*, Digitale systemer. (Listen er ikke udtømmende).

6.1.2 Når en stat står bag en cyberhændelse

Når det skal vurderes om en stat står bag en cyberhændelse, skal både sikrede og Tryg tage hensyn til objektive og rimelige beviser. Dette kan inkludere officielle udtalelser fra regeringer eller internationale sikkerhedsorganisationer som ENISA, nationale CERT myndigheder eller CISA.

Hvis der opstår uenighed, kan Tryg udpege en neutral ekspert til at træffe en bindende beslutning.

6.1.3 Begrænsninger relateret til geopolitiske forhold
Forsikringen dækker ikke skader, tab eller afbrydelser, der direkte eller indirekte skyldes eller udspringer af beslutninger, sanktioner, eksportkontrol, handelsrestriktioner eller andre foranstaltninger truffet af udenlandske stater, herunder – men ikke begrænset til – suspension, hel eller delvis ophør af adgang til software, tjenester eller infrastruktur leveret af udenlandske virksomheder som følge af geopolitiske forhold.

6.1.4 Forsikringen dækker herudover ikke skade som er en direkte følge af:
- Oversvømmelse fra hav, fjord, sø, å eller vandløb, herunder stormflod*.
- Jordskælv, tornadoer, vulkanudbrud eller andre natur- forstyrrelser.
- Beslaglæggelse, nationalisering eller revolution.
- Atomkernereaktioner og radioaktivt henfald, uanset om skaden sker i krigstid eller i fredstid. Forsikringen dækker dog skade, som skyldes eller sker i forbindelse med kernereaktioner, der bliver anvendt til sædvanligt industrielt, medicinsk eller videnskabeligt formål. Anvendelsen skal være forskriftsmæssig og må ikke stå i forbindelse med reaktor- eller acceleratordrift.

6.2 Forsikringen dækker ikke

- Enhver form for indirekte omkostninger eller tab, herunder renteudgifter, kontraktbøder, tab af goodwill samt tab som følge af mistede data* vedrørende fordringer, tilgodehavender og fakturabeløb.
- Betaling af løsesum eller nogen anden form for økonomisk udlæg i forbindelse med afpresning, herunder trusler relateret til cyberangreb eller cybersvindel.
- Indirekte tab, følgetab eller driftstab - medmindre forsikringen omfatter afsnit 5.2. Cyber Driftstab. Det fremgår af policen om dækningen er omfattet af forsikringen.
- Forsikringen dækker ikke omkostninger relateret til tid brugt på interne møder, planlægning, ineffektiv tid eller andre administrative aktiviteter, der opstår som følge af en dækningsberettiget skade. Dette inkluderer, men er ikke begrænser til, tid brugt af ledelse og medarbejdere på at koordinere respons, udarbejde rapporter eller deltage i møder vedrørende hændelsen.
- Enhver form for omkostninger til udskiftning af betalingskort, ID-papirer og lignende.
- Tyveri eller misbrug forårsaget af ansatte* eller personer, som sikrede har givet bemyndigelse til at benytte sikredes identitet.
- Enhver form for omkostninger eller tab, der opstår som følge af download af ulovlig software eller piratkopieret software.
- Betalingsanmodning efterkommet af sikrede i den tro, at anmodningen var fremsat af sikredes ledelse eller af en særligt betroet ansat - medmindre forsikringen er omfattet af afsnit 5.6 Cybersvindel. Det fremgår af policen om dækningen er omfattet af forsikringen.
- Enhver form for bøder eller tilsvarende, uanset om de tilfalder en privat eller en offentlig myndighed.
- Angreb, skade eller tyveri forårsaget af en person, der ejer mere end 5 procent af sikredes aktier eller anparter, eller som har været medlem af sikredes bestyrelse eller direktion/ faktisk ledelse, eller som udfører eller har udført arbejde for sikrede i egenskab af selvstændig revisor eller advokat. Dette gælder uanset om den pågældende handler alene eller i ledtog med andre.
- Omkostninger, som fabrikant, leverandør eller reparatør er ansvarlig for ifølge kontrakt, lov eller retspraksis, medmindre denne er gået konkurs, er under betalingsstandsning eller er under konkurslignende forhold.
- Begivenheder der fandt sted, inden forsikringen trådte i kraft, herunder software eller data*, der var tabt eller skadet, inden forsikringen trådte i kraft.
- Enhver form for fysisk skade på, herunder tyveri, ran, røveri og bortkomst af, sikredes IT-udstyr, IT-system eller netværk.
- Omkostninger til at fjerne softwarefejl, medmindre fejlen er en direkte følge af en i øvrigt dækningsberettiget skade.
- Omkostninger i forbindelse med indgåelse af aftaler, forlig, forhandlinger eller anden form for kontakt eller betaling til den eller de personer, der har stået bag angrebet, tyveriet eller misbruget.
- Omkostninger, der medfører, at sikrede er stillet bedre end før den dækningsberettigede begivenhed fandt sted, herunder opgraderinger eller forbedringer af software eller data*.
- Omkostninger eller tab som følge af angreb mod sikredes bankkonto, værdipapirdepot eller lignende, medmindre forsikringen er omfattet af afsnit 5.6 Cybersvindel. Det fremgår af policen om dækningen er omfattet af forsikringen.
- Omkostninger der skyldes svigt i el-, gas-, internet- eller anden form for energiforsyning, herunder ydelser leveret af teleudbydere.
- Enhver form for ansvar overfor tredjemand. Dog undtaget dækningen "Datatab - ansvar".
- Sikredes omkostninger til opgørelse af erstatningskrav eller konstatering eller sandsynliggørelse af en dækningsberettiget begivenhed.
- Sager om immaterielle rettigheder, herunder tvister om rettigheder til navne, designs, varemærker, ophavsret, patenter og domæner.

6.3 Forsikringen dækker ikke virksomheder, der udfører aktiviteter inden for følgende områder, medmindre andet fremgår af forsikringsaftalen.

- Trykning eller distribution af aviser, dagblade, ugeblade og lignende, uanset om det er fysisk eller digitalt.
- Postvæsen.
- Telekommunikation.
- Offentlig transport.
- Fremstilling af transportmidler.
- Programmering, vedligeholdelse eller distribution af software, herunder operativsystemer, applikationer, computerspil og anden software. Det betyder dog at simple automatiseringer og scripts, som makroer i Excel eller Visual Basic Script (VBS) der fx bruges til at lette arbejdsgange, ikke falder ind under de programmeringsaktiviteter der er undtaget.
- Online udbud af softwareprodukter eller computerspil.
- IT-, web-, server- eller anden form for hosting.
- Drift af online søgemaskiner.
- Drift af online datingservice eller aktivitet, der kan sidestilles hermed.

7. Hvis skaden sker

7.1 Skadebehandling

Tryg benytter i skadebehandlingen eksterne samarbejdspartnere, som er eksperter i behandling af skader, omfattet af denne forsikring.

Tryg udpeger den eller de eksperter, der skal:
- sikre rekonstruktion af dine IT-systemer, netværk, software eller data*
- foretage juridisk rådgivning i forbindelse med tab af data
- gennemføre nødvendig indberetning og underretning i forbindelse med tab af data

Tryg videregiver de nødvendige oplysninger om sikrede til den eller de eksperter, som Tryg har udpeget, så eksperterne er i stand til at behandle sikredes skade.

Eksperterne vil være selvstændigt dataansvarlige for de oplysninger, som eksperterne indsamler og registrerer om dig. Sikrede skal tage kontakt til den eller de eksperter, som Tryg har udpeget, hvis sikrede vil benytte retten til indsigt, gøre indsigelse mod behandlingen eller korrigere dine personlige oplysninger hos den eller de udpegede eksperter.

Sikrede er forpligtet til at følge de udpegede eksperters anvisninger, bistå med nødvendig dokumentation og oplysninger til brug for sagens behandling, samt samarbejde med os med henblik på at begrænse omkostningernes omfang.

Såfremt sikrede benytter anden IT-ekspert end vores eksterne samarbejdspartnere, til udbedring af skaden, vil disse omkostninger blive dækket med højst 35.000 kr. Tryg forbeholder sig retten til at gennemgå skadesagen med vores eksterne samarbejdspartner.

Sikrede er forpligtet til for egen regning at afholde udgifter til dokumentation af et erstatningskrav i form af revisionspåtegning, - opgørelse eller lignende, såfremt Tryg kræver dette.

7.2 Krav mod tredjemand

I det omfang Tryg har betalt en erstatning, indtræder Tryg i dit krav mod tredjemand.

8. Generelle bestemmelser

8.1 Forsikring i andet selskab

Hvis der er tegnet forsikring mod samme type af skade i et andet forsikringsselskab, foreligger der dobbeltforsikring, og skaden skal anmeldes til begge selskaber.

Tryg betaler ikke erstatning for skader, som der er modtaget fuld dækning for hos et andet forsikringsselskab. Har det andet selskab begrænset dækning i tilfælde af dobbeltforsikring, gælder de samme begrænsninger i denne forsikring. Dermed er Tryg og det andet forsikringsselskab forpligtede til at betale forholdsmæssig erstatning, hvis skaden er dækket af forsikringen.

8.2 Forsikrings varighed og opsigelse

8.2.1 Varighed
Forsikringens aftaleperiode fremgår af forsikringsaftalen.

Ved aftaleperiodens udløb fortsætter forsikringen uændret i en tilsvarende periode.

8.2.2 Opsigelse
Både sikrede og Tryg kan opsige forsikringen skriftligt med en måneds varsel til førstkommende (hoved)forfaldsdato.

8.2.3 Opsigelse ved skade eller tab
Når en skade eller tab er anmeldt, kan Tryg opsige eller indføre ændringer i forsikringen, herunder ændring i pris og selvrisiko, med 14 dages varsel. Opsigelsen eller ændringen i forsikringen kan indføres fra skaden eller tabet anmeldes og til senest 1 måned efter, at erstatningen er udbetalt eller skaden er afvist.

Hvis sikrede ikke godkender ændringen af forsikringen, kan forsikringen opsiges skriftligt inden ændringsdatoen. Sker dette ikke, betragtes ændringen som accepteret og forsikringen fortsætter på de ændrede vilkår.

Tryg kan opsige et kundeforhold, hvis kunden eller en person, der er berettiget til at disponere på kundens vegne, eller ejerkredsen, direkte eller indirekte, helt eller delvist er omfattet af finansielle sanktioner udstedt af EU, FN, OFAC eller andre relevante myndigheder i fx US og UK. Eventuelle udbetalinger vil blive indefrosset indtil det er muligt at udbetale.

8.3 Forsikringens betaling

Forsikringen betales en eller flere gange om året. Det fremgår af forsikringsaftalen, hvad der er valgt.

Første betaling til os skal betales, når forsikringen træder i kraft. Senere opkrævninger skal betales på de forfalds- eller ændringsdatoer, som fremgår af forsikringsaftalen. Udover forsikringens pris opkræves eventuelle afgifter, for eksempel skadeforsikringsafgift og statsafgift samt gebyrer, morarenter og andre omkostninger.

Tryg opkræver betalingen via Betalingsservice, indbetalingskort eller efter aftale på anden vis. Opkrævningen sendes til den betalingsadresse, Tryg er blevet oplyst. Hvis betalingsadressen ændres, skal Tryg straks have besked.

Hvis forsikringen ikke betales senest sidste rettidige indbetalingsdag, sender Tryg en rykkerskrivelse med oplysning om, at forsikringens dækning ophører, hvis forsikringen ikke betales senest 21 dage efter, at rykkerskrivelsen er sendt.

8.4 Gebyrer

Tryg er berettiget til at beregne gebyrer til hel eller delvis dækning af omkostningerne ved fx opkrævninger, rykkerskrivelser, inkasso, udpantning, udbetalinger, print og behandling af dokumenter, oversigter, besigtigelser, ekspeditioner og ydelser i forbindelse med forsikrings- og skadebehandling.

Tryg kan ændre eksisterende gebyrer eller indføre nye gebyrer, når det er begrundet i;

- Omkostningsmæssige årsager – fx hvis flere processer eller ydelser digitaliseres, eller der indføres flere selvbetjeningsløsninger
- Forretningsmæssige årsager – fx for at udnytte ressourcer eller kapacitet på en mere hensigtsmæssig måde, eller for at ændre den generelle gebyrstruktur
- Markedsmæssige årsager – fx hvis grundlaget for gebyret har ændret sig, eller hvis kundeadfærd ændres.

Nye gebyrer og ændringer af eksisterende gebyrer varsles via vores hjemmeside med 1 måneds varsel til den første dag i en måned.

Tryg kan uden varsel sætte gebyrer ned.

Gældende gebyrer vil altid fremgå af www.tryg.dk eller oplyses ved henvendelse til Tryg.

8.5 Indeksregulering

Indeksregulering følger "lønindeks for den private sektor", der er udregnet af Danmarks Statistik. Ophører udgivelsen af dette indeks, eller ændres grundlaget for beregningen, har Tryg ret til at benytte et lignende indeks fra Danmarks Statistik.

Selvrisici indeksreguleres, medmindre andet fremgår af forsikringsbetingelserne eller forsikringsaftalen. Indeksreguleringen sker hvert år den 1. januar.

Prisen indeksreguleres en gang om året på forsikringens første betalingsdag i kalenderåret.

8.6 Præmieregulering og ændring af forsikringsbetingelser

Ændring af prisen for forsikringen, som ikke er begrundet i ændringer i lovgivningen eller indeksregulering, skal varsles skriftligt senest 1 måned før forsikringens hovedforfaldsdato.

Ændring af forsikringsbetingelserne, der ikke er begrundet i ændringer i lovgivningen og/eller som blot har præciserende karakter, skal varsles skriftligt senest 1 måned før forsikringens hovedforfaldsdato.

Hvis sikrede ikke ønsker at acceptere de varslede ændringer, skal forsikringen opsiges skriftligt senest 14 dage inden ændringsdatoen. I modsat fald fortsætter forsikringen på de ændrede vilkår og/eller til den ændrede pris.

8.7 Ansvarlige forretningsprincipper

Tryg forventer, at sikredes ejere og medarbejdere driver den sikrede virksomhed i overensstemmelse med ansvarlige forretningsprincipper som beskrevet i FN Global Compacts ti principper. Det betyder, at Tryg forventer, at sikrede virksomhed respekterer menneskerettigheder, opretholder ordentlige arbejdsforhold, arbejder for at minimere negativ miljø- påvirkning og for at modarbejde alle former for korruption.

Læs mere her:
De Ti Principper - Global Compact Network Denmark

8.8 Sikredes forpligtelser

Når der indtræffer en dækningsberettiget skade, skal sikrede uden ophold og efter bedste evne forsøge at begrænse skaden.

9. Moms

Moms i henhold til gældende lovgivning bæres af sikrede i det omfang, sikrede kan trække beløbet fra sit momsregnskab over for Skat.

Tryg udlægger ikke momsbeløb.

10. Lovvalg og værneting

Tvister vedrørende forsikringsaftalen afgøres efter dansk ret ved danske domstole.

11. Ordforklaring

Hvor der i de enkelte afsnit er anført en * er emnet uddybet i nedenstående ordforklaring

Adgangskode
Med en stærk adgangskode menes en kode, som indeholder mindst 14 tegn, heraf både store og små bogstaver samt tal, og at denne skiftes minimum hver 12 måned. Adgangskoden må ikke indeholde navnet på sikrede, og må ikke være identisk med eller have stor lighed med brugernavn eller kodeord, som benyttes af andre hos sikrede. Tryg anbefaler multifaktorgodkendelse MFA*.

Ansatte
Enhver lønnet person, herunder trainees og konsulenter som arbejder under en kontrakt i din tjeneste.

Backup
En backup er en kopi af sikredes data, der gemmes et sikkert sted for at beskytte mod tab og skade. Hvis de originale data går tabt, kan de gendannes fra backuppen.

Tryg anbefaler at anvende 3-2-1 backup-reglen af sikredes data. Herved kan data hurtigt kan genskabes og gendannes efter en dækningsberettiget skade. Reglen foreskriver at opbevare 3 kopier af sikredes data. På mindst 2 forskellige lagringsmedier. Hvor mindst 1 af kopierne er placeret et andet sted end sikredes netværk.

BEC
BEC, eller Business Email Compromise, er en form for cyberkriminalitet, hvor svindler fx bruger e-mails til at narre medarbejdere til at sende penge. Svindler udgiver sig ofte for at være en betroet person eller virksomhed.

Biometri
Biometri er brugen af biologiske målinger eller fysiske karakteristika, såsom fingeraftryk, ansigtsgenkendelse eller iris-scanning, til at identificere og verificere en persons identitet.

CEO-fraud
CEO-fraud er en type svindel, hvor svindler udgiver sig for at være sikredes CEO, eller en anden højtstående leder, med det formål at svndle medarbejdere til at overføre penge.

Cyberkrig
Cyberkrig, refererer til en bredere konflikt hvor der anvendes digitale angreb, der kan og ofte har til formål, at forårsage omfattende skade på it-infrastruktur og data hos sikrede. Angreb som disse kan resultere i betydelige økonomiske tab for sikrede.

Cyberkrigsførelse
Cyberkrigsførelse, refererer til brugen af digitale teknologier eller udstyr, til udførelse af angreb med det formål at forstyrre, sabotere, manipulere, destruere, eller gøre skade. Dette omfatter blandt andet hacking, malware, spredning af skadelig software som virus, DDoS-angreb*, eller udførelse af misinformative informationskampagner fx på sociale medier.

Cyberoperation
Cyberoperation, refererer til enhver handling udført af en stat eller dens agenter, med det formål at forstyrre, nægte adgang til, manipulere eller ødelægge informationssystemer, digitale strukturer, kritisk infrastruktur eller andre essentielle tjenester.

Data
Data og programmer, der kan indlæses i en computer, herunder softwaremæssig systemopsætning. Dog betragtes data i lukkede (ikke redigerbare) elektroniske kredsløb (IC-kredse) ikke som data.

Databehandler
Med en databehandler forstås en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

Datterselskab
Som datterselskab anses juridiske personer (selskaber) i hvilke sikrede selv, eller sammen med andre sikrede, besidder mere end 50% af stemmerettighederne.

DDoS
DDoS står for Distributed Denial of Service, og ligesom DoS, der står for Denial of Service, refererer begge begreber til angreb, der har til formål at overbelaste og lamme et system. Forskellen er, at et DoS-angreb typisk udføres af én enhed, mens et DDoS-angreb involverer flere enheder, ofte spredt over forskellige netværk.

DKIM
DKIM (DomainKeys Identified Mail) er en e-mail autentificeringsmetode, der bruger kryptografiske signaturer til at verificere at en e-mail virkelig kommer fra det domæne den hævder at komme fra. Det sikrer også, at e-mailens indhold ikke er blevet ændret undervejs.

DMARCH
DMARCH (Domain-based Message Authentication, Reporting & Conformance) er en e-mail autentificeringsprotokol der fortæller modtagende e-mail servere hvad de skal gøre, hvis en e-mail ikke består SPF eller DKIM. DMARCH kan instruere servere til at afvise, sætte i karantæne eller levere e-mails baseret på autentificeringsresultater.

Domæne:
Et domæne er en unik adresse der bruges til at identificere og tilgå en specifik website på internettet.
Et domæne inkluderer både domænenavnet og den tekniske struktur bag navnet.

Domænenavn
Et domænenavn er den tekstbaserede adresse der identificerer et domæne.

EDR-software* (Endpoint Detection and Respons) er en software der overvåger og analyserer data aktiviteten. EDR-software er en avanceret antivirus-software der identificerer sikkerhedsbrud i realtid og kommer med en meget hurtigt reaktion på truslen. EDR er en moderne cybersikkerheds teknologi, da den hjælper med at beskytte sikrede mod avancerede trusler som ransomware og andre former for malware.

Elektronisk indbrudstyveri
Ved elektronisk indbrudstyveri forstås, at personer, der ikke er ansat hos sikrede, stjæler penge ved at tiltvinge sig adgang via netbank i et dansk pengeinstitut til sikredes bankkonto, uanset om den berørte konto er placeret i et dansk eller udenlandsk pengeinstitut.

Fakturasvindel
Fakturasvindel er en form for økonomisk kriminalitet, hvor svindlere forsøger at narre sikrede til at betale falske fakturaer. Dette kan ske ved, at svindlerne udgiver sig for at være en legitim leverandør og sender en faktura med falske betalingsoplysninger. Målet er at få sikrede til at overføre penge til svindlernes konto i stedet for den rigtige leverandørs konto.

Forretningskritiske data
Forretningskritiske data omfatter finansielle oplysninger, kunde- og leverandørinformation, fortrolige strategier, adgangsoplysninger og driftskritiske systemer. Disse data er afgørende for sikredes drift og økonomiske eksistens.

Fysisk har sikret adgangen
Ved at sikrede fysisk har sikret adgangen menes, at virksomhedens IT-udstyr herunder computere, servere, routere mv. som minimum skal befinde sig i aflåst bygning og lokale udenfor virksomhedens åbningstid.

Hackerangreb
En ulovlig indtrængen i IT-systemet begået af en person, der ikke er ansat (se også under "Virus").

Hybridkrig
Hybridkrig, refererer til en kombination af angrebsmetoder der anvendes samtidig, eller forskudt af hinanden – og som er medvirkende til at skabe forvirring og udnytte sårbarheder.

ID-tyveri
ID-Tyveri defineres som situationer hvor virksomhedsoplysninger misbruges, uden samtykke fra sikrede, og uberettiget bliver brugt af en anden/andre personer/virksomheder med henblik på økonomisk svindel.

IoT-enheder
IoT, eller Internet Of Things, er fysiske objekter der er forbundet til internettet, og som kan indsamle, sende og modtage data.

Juridisk bistand
Med juridisk bistand forstås nødvendige og rimelige udgifter til juridisk rådgivning eller repræsentation til beskyttelse af sikredes interesser i forbindelse med en forsikret begivenhed.

Kryptovaluta
Kryptovaluta er en digital valuta, der bruger kryptografi til sikkerhed og fungerer uden en central myndighed som bank. Eksempler inkluderer Bitcoin og Ethereum, som blandt andet bruges til betalinger, investeringer.

MFA (Multifactor Authentication)
Multifaktorgodkendelse, i daglig tale MFA, er en sikker metode til at logge på netværk, systemer, programmer og servere med videre. MFA tilføjer et ekstra lag af sikkerhed ved at kræve, at brugeren bekræfter sin identitet med to eller flere faktorer.

NBCR-terrorskader
NBCR-terrorskader refererer til skader forårsaget af terrorangreb, der involverer nukleare, biologiske, kemiske eller radiologiske (NBCR) våben.

Netværk
Omfatter mobile enheder, USB-nøgler, sikredes netværk og andre databærende medier.

OT-enheder
OT-enheder står for Operationel Teknologi-enheder. Disse enheder omfatter hardware og software der bruges til at overvåge og styre processer og fysiske enheder.

Personoplysninger
Med personoplysninger forstås enhver form for information, der kan henføres til bestemte personer, eksempelvis personnummer, billede, registreringsnummer eller lignende.

Phishing
Phishing refererer til cyberangreb, hvor angriberen forsøger at narre medarbejdere til at afsløre følsomme oplysninger som adgangskoder, kreditkortnumre eller andre personlige data. Dette sker typisk gennem falske e-mails, beskeder eller websites, der ser ud til at komme fra en troværdig kilde.

Privatrelateret svindel
Privatrelateret svindel retter sig typisk direkte mod enkeltpersoner, og omfatter svindel som Love Scam (romantisk svindel), Arvesvindel, phishing og identitetstyveri. Forskellen på erhvervsmæssig svindel og privatrelateret svindel er primært metoden og målgruppen. Den privatrelaterede svindel spiller ofte mere på følelser, tillid og frygt, hvor den erhvervsrelaterede svindel typisk er mere strategisk og manipulerende.

Ransomware
Angreb udført med det formål at inficere sikredes PC'ere og krypterer brugernes filer og dokumenter. Herefter kræver hackerne løsepenge for at frigive filerne og dokumenterne igen.

Regelmæssigt (skift af adgangskode)
Med regelmæssigt menes, at adgangskoden ændres hver 12. måned. På den måde minimeres sandsynligheden for, at den kode som en kriminel måtte få fat i, faktisk fungerer. Jo oftere koden skiftes, desto mindre er sandsynligheden for, at den kode en hacker har fået fat i, er den nyeste.

Social engineering
Social engineering er en metode, hvor svindlere manipulerer mennesker til at afsløre fortrolige oplysninger eller udføre handlinger, der kan kompromittere sikkerheden. Dette kan blandt andet ske via telefonopkald, SMS eller e-mail, hvor svindleren - i stedet for at bruge tekniske hackingmetoder - udnytter menneskers psykologi og tillid.

SPF
SPF (Sender Policy Framework) er en e-mail autentificeringsmetode, der hjælper med at forhindre at svindlere sender e-mails på vegne af sikredes domæne. Dette gøres ved at identificere hvilke servere der har tilladelse til at sende e-mails fra sikrede domæne.

Stormflod
Ifølge lov om erstatning af skader forårsaget af stormflod kan der via Naturskaderådet, der er nedsat af staten, under visse forudsætninger ydes erstatning for skade på fast ejendom og løsøre efter oversvømmelse opstået som følge af ekstrem højvandstand i havet forårsaget af storm.

Terrorisme
Ved terrorisme forstås en handling, herunder - men ikke begrænset til - vold eller trussel om anvendelse af vold, foretaget af en person eller flere personer, uanset om de handler på egen hånd eller i forbindelse med en eller flere organisationer og/eller myndigheder, begået med politisk, religiøst, ideologisk eller etnisk formål eller begrundelse, herunder med den hensigt at påvirke en regering og/eller at sprede frygt i offentligheden eller dele af offentligheden.

For at karakterisere handlingen som terrorisme forudsættes, at handlingen er egnet til at påvirke en regering og/eller sprede frygt i offentligheden eller dele deraf.

Tort-godtgørelse
Særlig godgørelse for krænkelse eller ydmygelse som tilføjes en person, så denne mister anseelse eller selvfølelse.

Virus
Ved virus forstås et program, der er udviklet til at sprede sig selv med den hensigt at påvirke eller skade indholdet i andre programmer, som ofte derved ødelægges. Et virusangreb er således forårsaget af en automatisk proces, der er blevet initieret fx ved, at en medarbejder hos sikrede har klikket på fx et link i en mail, klikket på et link på en hjemmeside mv.

Website defacement
Ved et website defacement-angreb, får en hacker adgang til en hjemmeside, og lægger sine egne sider ind på den.

Website hijacking
Ondsindet/uautoriseret overtagelse af sikredes hjemmeside eller programmer, der installeres på din computer via virus*, med det formål at overtage kontrollen med hjemmesiden.