Zurich Cyber

Aanvraagformulier

Instructies

Geef alstublieft volledig antwoord op elke vraag

Wanneer het formulier onvoldoende ruimte biedt, levert u de informatie dan separaat aan.

Het aanvraagformulier en separate informatie dient volledig, getekend en gedateerd te zijn door een bestuurder of daartoe bevoegd persoon.

Het invullen en indienen van dit aanvraagformulier geeft geen verplichting tot het aangaan van een verzekering. Om ervoor te zorgen dat er zo min mogelijk aanvullen informatie gevraagd dient te worden vragen wij u de vragen volledig te beantwoorden.

Verzekeraars gaan ervan uit en mogen erop vertrouwen dat een representatieve weergave van het risico wordt gegeven doormiddel van het invullen van dit formulier. Dit houdt in dat aanvrager gehouden is informatie te voorzien van feiten en omstandigheden die van materiele aard zijn voor het risico dat wordt gedekt door de aangevraagde verzekering. Een feit of omstandigheid van materiele aard is er één waarvan het aannemelijk is of waarvan men kan verwachten die van invloed zijn op de acceptatie en/of beoordeling van het risico. Als hierover twijfel bestaat is het in uw belang deze feiten en omstandigheden mede te delen.

1. Algemene informatie

Volledig naam onderneming (Moeder bedrijf):

Hoofd-adres (HQ) (Voeg alstublieft een volledig organogram incl. omzetsplit per land indien van toepassing bij)

Jaar Oprichting

Aantal werknemers:

Website

Volledige omschrijving van de bedrijfsactiviteiten:

Zijn er andere ondernemingen geworven, gefuseerd of samengegaan met de aanvrager de afgelopen 2 jaar? ☐ Yes ☐ No

Zo Ja, is de IT-integratie volledig afgerond? ☐ Yes ☐ No

Zo nee, lever details aan:

Huidige omzet (laatste 12 maanden), eindigend D D M M Y Y Y Y € _____

Verwachte omzet (komende 12 maanden), D D M M Y Y Y Y € _____

Netto winst (laatste financiele jaar) € _____

Territory	Percentage Omzetsplit (%)
Nederland	
UK	
Europe (exclusief UK)	
USA	
Rest of the World	

Percentage van de omzet dmv website of ecommerce platform _____

Section 1. Additionele opmerkingen

2. Identificeren

a) Geschat aantal unieke records/data tav persoonsgegevens toevertrouwd aan de zorg van de aanvrager:

PII Persoonsgegevens (inclusief gegevens van werknemers)	
Payment card details (opgeslagen op het netwerk)	
Payment card details (jaarlijks geprocessed)	
Persoonlijke financiele informatie (anders dan creditcard gegevens)	
Healthcare information	
Government identification (BSN, passport, rijbewijs, social security, etc.)	

b) Is er een hardware en data inventarisatie uitgevoerd in de laatste 2 jaar? ☐ Yes ☐ No

c) Onderhoudt de organisatie een Data Security Policy met daarin een data classificatie standaard? ☐ Yes ☐ No

d) Welk % van het jaarlijkse IT budget is gealloceerd aan Informatie beveiliging ? _____

e) Heeft de organisatie een Security and Privacy Awareness programma met minimaal verplichte deelname voor alle gebruiker? ☐ Yes ☐ No

f) Voert de organisatie jaarlijks phishing simulaties uit voor alle on all users on at least an annual basis? ☐ Yes ☐ No

g) Staat de organisatie Bring-Your-Own-Device toe? ☐ Yes ☐ No

h) Heeft uw organisatie de mogelijkheid tot het op afstand wissen van mobile devices? ☐ Yes ☐ No

i) Geef een opsomming van bedrijfskritische IT, OT, Cloud Service Providers en Business Process Outsourcers tezamen met de services (e.g. Managed Security Services, Cloud/Backup/Website Hosting, Internet Service Providers, Bedrijfs kritische Software Providers, Data Processors, POS Hardware Providers, Colocation Services):

Provider	Service	RTO	Schade per uur

i) Bevatten alle contracten van toeleverancier de volgende bepalingen:

i) Verplichting voor leverancier voor het tijdig melden van cyber en/of privacy incidenten In overeenstemming met lokale wet en regelgeving? ☐ Yes ☐ No

ii) Vrijwaring van de aanvrager voor aansprakelijkheid (inclusief notificatie kosten) als gevolg van een Network- of privacy incident die aan leverancier is toe te rekenen? ☐ Yes ☐ No

j) Hoe vaak worden toegangsrechten gecontroleerd? _____

k) Worden leveranciers gecontroleerd of ze voldoen aan beveiligingsstandaarden van de aanvrager? ☐ Yes ☐ No

Zo nee, welke controle vindt plaats voordat met een leverancier wordt gecontracteerd?

_____

m) Verkoopt of deelt aanvrager persoonsgegeves met/aan derden? ☐ Yes ☐ No

Zo ja:

i) Zijn betrokkenen daarover geinformeerd en een kans geboden om af te zien van gebruik van die informatie door derden? ☐ Yes ☐ No

ii) Contracteert aanvrager met de betreffende leveranciers de gebruikers voorwaarden die gelijk of beter zijn dan de eigen voorwaarden? ☐ Yes ☐ No

n) Gebruikt u 'end of life systems' zoals Windows XP? ☐ Yes ☐ No

Zo ja, hoe mitigeert u dit risico?

_____

Section 2. Additional Comments

3. BEVEILIGEN:

a) Zijn alle persoonsgegevens en/of andere gevoelige informatie:

Encrypted bij opslag ☐ Encrypted op draagbare media (incl USBs en laptops) ☐

Encrypted onderweg ☐ Gesegmenteerd van het overige netwerk ☐

b) Is het volgende geinstalleerd op alle werkstations en laptops?

Intrusion prevention software	☐ Yes	☐ No
Intrusion detection software	☐ Yes	☐ No
Data loss prevention software	☐ Yes	☐ No
Anti-virus software	☐ Yes	☐ No

c) Is de aanvrage PCI gecertificeerd: ☐ Yes ☐ No

Zo ja, welk merchant level ☐ 1 ☐ 2 ☐ 3 ☐ 4

d) Bestaat er een formeel proces voor het principe van "least privilege" voor toegang van individuen tot bedrijfssystemen en applicaties? ☐ Yes ☐ No

e) Hebben alle administrators separate persoonlijke en administrator accounts? ☐ Yes ☐ No

f) How often are individual access rights reviewed for appropriateness? _____

g) Verwijderd u toegang direct na beeindiging van een contract dienstverband voor werknemers en/of dienstverleners? ☐ Yes ☐ No

h) Is multifactor authentication (MFA) vereist voor :

(Remote) externe toegang tot uw netwerk	☐ Yes	☐ No
Toegang tot administrator accounts	☐ Yes	☐ No
Toegang tot uw network door dienstverleners en derden	☐ Yes	☐ No

i) Heeft u een geformaliseerd beleid voor het verwijderen van data en documenten wanneer die niet lander nodig zijn voor uw organasatie? ☐ Yes ☐ No

j) Heeft u minimum vereisten voor paswoord complexiteit? ☐ Yes ☐ No

k) Heeft u firewalls op alle externe toegangspunten? ☐ Yes ☐ No

l) Gebruikt u de volgende email beveiligingsframeworks?:

SPF	☐ Yes	☐ No
DMARC	☐ Yes	☐ No
TLS	☐ Yes	☐ No

m) Maakt u gebruik van een cloud email-oplossing (zoals Office 365)? ☐ Yes ☐ No

Zo ja, maakt u gebruik van multifactor authentication (MFA) voor toegang? ☐ Yes ☐ No

Section 3. Additional Comments

4. DETECTEREN:

a) Gebruikt u een 24x7 security monitoring oplossing van het network doormiddel van eigen personeel of door een Managed Security Services Provider? ☐ Yes ☐ No

b) Log management:

i) Maakt u gebruik van een Security Information and Event Management product (SIEM)? ☐ Yes ☐ No

ii) Hoe vaak worden de logs gecontroleerd? _____

iii) Wat is de verwachte response tijd voor een bedrijf kritisch alarm? _____

c) Heeft u beleid geïmplementeerd om regelmatig uw systemen en applicaties te patchen, gebaseerd op de mate hoe kritisch deze zijn voor uw bedrijfsprocessen? ☐ Yes ☐ No

d) Binnen welke tijd verricht u kritische / high vulnerability patches? _____

e) Hoe vaak worden beveiligingsaudits of penetratie testen door derden verricht op uw netwerk? _____

f) Zijn er uitstaande kritische aanbevelingen die geimplementeerd dienen te worden op basis van recente beveiligingsaudits of penetratie testen? ☐ Yes ☐ No

Zo ja, graag informatie over de te nemen acties en planning voor implementatie

Section 4. Additionele Opmerkingen

---

5. REAGEER:

a) Heeft u direct 'incident response' capaciteit in huis ofwel door een Managed Security Services Provider? ☐ Yes ☐ No

b) Heeft uw organisatie een gedocumenteerd Incident Response plan? ☐ Yes ☐ No

i) Zijn duidelijke rolverdelingen en verantwoordelijkheden gedefinieerd in het plan? ☐ Yes ☐ No

ii) Bevat het plan "playbooks" voor specifieke incidenten (zoals: ransomware, DDoS, verlies van data, etc.)? ☐ Yes ☐ No

iii) Wordt het plan minimal jaarlijks getest en geupdate? ☐ Yes ☐ No

Section 5. Additionele opmerkingen

---

6. Herstel:

a) Heeft uw organisatie een gedocumenteerd Disaster Recovery and Business Continuity plan? ☐ Yes ☐ No

b) Hoe vaak worden deze getest en geupdate? _____

c) Wat zijn uw Recovery Time Objectives (RTOs)

	Recovery Time Objectives
Critical systems	
Non-critical systems	

d) Hoe vaak worden kritische systemen en data backed up (dagelijks, wekelijks, etc.)? _____

e) Hoe vaak wordt niet kritische data en systemen backed up (dagelijks, wekelijks, etc)? _____

f) Waar wordt backed up data opgeslagen (zoals tapes, cloud, etc.)

_____

g) Zijn uw backups fysiek disconnected en niet toegankelijk van uw ? ☐ No ☐ Yes

h) Zijn bedrijfskritische systemen gedupliceerd en in een offline en redundante omgeving ☐ No ☐ Yes

i) What workarounds are available to minimise the financial impact of a network interruption?

_____

Section 6. Additional Comments

7. Aanvrager historie

a) Is aanvrager in de laatste drie jaar een gelijke verzekering gewijgerd of opgezegd ☐ Yes ☐ No

If Yes, please describe: _____

b) Heeft de aanvrager in de laatste 5 jaar een claim en/of schade geleden als gevolg van een data verlies, aanval op het computer systeem, Cyber ransom, onderzoek door toezichthouder voor schending van privacy recht of systeemuitval oid? ☐ Yes ☐ No

Zo ja, graag toelichting: _____

c) Heeft de aanvrager kennis van feiten en/of omstandigheden die kunnen leiden tot een schade, verlies en/of aanspraak op een verzekering als waarvoor nu een aanvraag voor wordt gedaan? ☐ Yes ☐ No

Zo ja, graag toelichting: _____

Section 7. Aanvullende opmerkingen

8. Internet Media Aansprakelijkheid

a) Publiceert de aanvrager blogs, newsberichten, videos, podcasts of andere content online? ☐ Yes ☐ No

b) Heeft de aanvragen een process om alle content te controleren voorafgaand aan publicatie online? ☐ Yes ☐ No

Zo ja, wordt de controle uitgevoerd door een jurist? ☐ Yes ☐ No

c) Publiceert de aanvrager content van derden op haar website? ☐ Yes ☐ No

Zo ja, graag een toelichting over de procedures er zijn voor het monitoren en/of aanpassen van content gepubliceerd op uw website inclusief uw "take down" voorwaarden.

9. Ondertekening

Het door de verzekeringnemer en/of verzekerde ingevulde en ondertekende aanvraagformulier en de overige verstrekteinlichtingen en verklaringen, in welke vorm dan ook, zijn de grondslag van de verzekeringsovereenkomst en vormen daarmee één geheel. Ondergetekende(n) verklaart (verklaren) bevoegd te zijn namens de rechtspersoon te tekenen en bevestigt (bevestigen), mede gelet op de inhoud van artikel 7:928 BW, dat de gegeven antwoorden en verklaringen juist en volledig zijn en dat mededeling is gedaan van de feiten en omstandigheden die voor Zurich van belang zijn voor de beoordeling van zowel het te verzekeren risico als ten aanzien van de verzekeringnemer en verzekerden.

Handtekening

Date D D M M Y Y Y Y

Naam

Positie

Toelichting
Als aanvrager/kandidaat-verzekeringnemer bent u verplicht de gestelde vragen in dit aanvraagformulier zo volledig mogelijk te beantwoorden. Dit geldt ook voor feiten en omstandigheden die betrekking hebben op een bij het sluiten van deze verzekering bekende derde, wiens belangen worden meeverzekerd. Bij de beantwoording is bovendien niet alleen de eigen wetenschap van aanvrager bepalend, maar ook die van de andere belanghebbende bij deze verzekering. Vragen waarvan u het antwoord al bij Zurich bekend veronderstelt, moet u toch ook zo volledig mogelijk beantwoorden. Feiten en omstandigheden die u bekend worden nadat u deze aanvraag heeft ingezonden, maar voordat Zurich u heeft bericht over zijn definitieve beslissing het door u ter verzekering aangeboden risico al dan niet te verzekeren, met u alsnog aan Zurich meedelen, indien deze vallen onder de vraagstelling in het aanvraagformulier. Indien u niet volledig aan uw mededelingsplicht heeft voldaan, kan dat ertoe leiden dat het recht op uitkering wordt beperkt of zelfs vervalt. Indien u met opzet tot misleiden van Zurich heeft gehandeld of deze bij kennis omtrent de ware stand van zaken de verzekering nummer zou hebben gesloten, heeft Zurich teven het recht de verzekering op te zeggen. In geval van fraude zal Zurich aangifte doen bij de politie, hetgeen kan leiden tot rechtsvervolging. Het door verzekeringnemer ingevulde en ondertekende aanvraagformulier en de overige verstrekte inlichtingen en gedane verklaringen, in welke vorm dan ook, zijn de grondslag van de verzekering en vormen daarmee één geheel."

Persoonsgegevens
Bij de aanvraag van een verzekering en/of financiële dienst worden persoonsgegevens en eventuele andere gegevens gevraagd. Deze worden door Zurich verwerkt ten behoeve van het aangaan en uitvoeren van verzekeringen en/of financiële diensten en het beheren van de daaruit voortvloeiende relaties, met inbegrip van de voorkoming en bestrijding van fraude en het uitvoeren van activiteiten gericht op de vergroting van het cliëntenbestand. Op de verwerking is de gedragscode "Gedragscode Verwerking Persoonsgegevens Financiële Instellingen" van toepassing. Deze gedragscode ligt op het kantoor van Zurich ter inzage.

ZURICH®