AANVRAAGFORMULIER ICT Bedrijven

Voor welke verzekering wenst u een offerte te ontvangen?

☐ Beroepsaansprakelijkheidsverzekering (BAV) ☐ Cyberverzekering

☐ Aansprakelijkheidsverzekering Bedrijven (AVB)

I Algemene informatie

Naam verzekeringnemer	
Adres	
Postcode en plaats	
Datum van oprichting	
Mee te verzekeren deelnemingen	
Website	

1. Heeft verzekeringnemer en/of een mee te verzekeren deelneming buitenlandse vestigingen? ☐ Ja ☐ Nee

Zo ja, in welke landen	

2. Heeft u thans een:
   a. Beroepsaansprakelijkheidsverzekering? ☐ Ja ☐ Nee
   b. Aansprakelijkheidsverzekering Bedrijven (AVB) ☐ Ja ☐ Nee
   c. Cyberverzekering? ☐ Ja ☐ Nee

II Jaaromzet - Landen

	Vorig boekjaar	**Dit boekjaar (prognose)**	**Volgend boekjaar (prognose)**
Nederland	€	€	€
USA/Canada (export*)	€	€	€
USA/Canada (lokaal**)	€	€	€
Overige landen	€	€	€
Totaal	€	€	€

* Onder “export” wordt verstaan de omzet die is gegenereerd door uw vestiging(en) buiten de USA of Canada, maar voortvloeiende uit overeenkomsten met opdrachtgevers die zich wel in de USA of Canada bevinden

** Onder “lokaal” wordt verstaan de omzet die is gegenereerd door uw lokale vestiging(en) binnen de USA of Canada en voortvloeiende uit overeenkomsten met opdrachtgevers die zich eveneens in de USA of Canada bevinden

1. Over welke boekjaren heeft u de laatste drie jaar een positief financieel resultaat behaald?

_____

III Jaaromzet - Producten en diensten

Hardware	Circa	**Software & diensten**	Circa	**Telecom & Netwerk diensten**	Circa
Servers	%	Pakket software - derden	%	Advies	%
PC’s	%	Pakket software - zelf ontwikkeld	%	Installatie	%
Randapparatuur	%	Maatwerk software	%	Beheer	%
Mobiele telefoons	%	Saas	%	Overige:	
Overige:		Advies	%		%
	%	Implementatie	%		%
	%	Detachering	%		%
	%	Hosting	%		%
	%	Overige:			%
	%		%		%

1. Welk percentage van de omzet wordt verkregen van (Semi-) overheidsinstellingen?

_____%

2. Heeft u 3 of meer individuele contracten met (Semi-) overheidsinstellingen per jaar? ☐ Ja ☐ Nee

IV Werknemers

1. Aantal : Nederland _____ Buitenland _____
2. Jaarloon: € _____ (aan de belastingdienst opgegeven bruto jaarloon)

V Overnames

1. Heeft u de laatste 18 maanden bedrijven overgenomen? ☐ Ja ☐ Nee

   Indien ja, graag een toelichting.

VI Opdrachtgevers

1. Welke producten en diensten levert u op de volgende gebieden :

   Luchthavens/Luchtvaartmaatschappijen, Gokken, Militaire geleidingssystemen, Massa vervoer, Data aggregation, Online beurzen, Handelsplatformen, Satellieten, Erotische content, Sociale netwerken, Nutsbedrijven, Beveiliging, Bankieren/Financiele transacties Gezondheidszorg, ERP/CRM/ SCM/EAI.

Per product en dienst graag ook het % van de omzet vermelden

Indien u geen enkel product of dienst op deze gebieden levert, graag aangeven met “geen”.

2. Welke nieuwe producten of diensten bent u van plan de komende 12 maanden te gaan leveren?

   Indien er geen wijzigingen zullen plaatsvinden graag aangeven met “geen”.

VII Contracten

1. Hoe vaak sluit u overeenkomsten met uw opdrachtgevers op basis van:

	Circa % van de jaaromzet
Uw eigen algemene leveringsvoorwaarden	%
Inkoopvoorwaarden van uw opdrachtgevers	%
Maatwerk voorwaarden	%
Anders, namelijk:	%

2. Accepteert u aansprakelijkheid voor gevolgschade, exclusief intellectueel eigendom en lichamelijk letsel ? ☐ Ja ☐ Nee

   Indien ja, tot welk bedrag beperkt u uw aansprakelijkheid voor gevolgschade, behalve in geval van intellectuele eigendomschade en personenschade;

   % van de contracten:

   a. Lager dan de contractwaarde _____%
   b. Gelijk aan contractwaarde _____%
   c. Hoger dan de contractwaarde _____%
   d. Geen beperking _____%
   e. Totaal 100 %

3. Omvang van de contracten:

   a. Gemiddelde contractwaarde € _____
   b. Looptijd gemiddeld contract _____ maanden
   c. Looptijd langste contract _____ maanden

4. Gegevens van de drie grootste contracten in de laatste drie jaar:

	1.	2.	3.
Naam opdrachtgever			
Beschrijving product/dienst			
Totale contract waarde	€	€	€
Ingangsjaar contract			
Totale duur contract	mnd	mnd	mnd
*Ontwikkelingsperiode**	*mnd*	*mnd*	*mnd*
*Implementatieperiode**	*mnd*	*mnd*	*mnd*
*Onderhoudsperiode**	*mnd*	*mnd*	*mnd*
Ontwikkeling	%	%	%
Licentie inkomsten	%	%	%
Consultancy/implementatie	%	%	%
Onderhoud	%	%	%
Hardware	%	%	%
Algemene voorwaarden**			

* Indien van toepassing

** Bijvoorbeeld uw voorwaarden, inkoopvoorwaarden opdrachtgever, maatwerk, etc.

5. Welke percentage van uw contracten:
   a. Dienen te worden beoordeeld door een terzake deskundige jurist en/of senior management _____%
   b. Bevatten:
      1. Een zogenaamde “Entire Agreement Clause” _____%
      2. Vrijwaringsbedingen _____%
      3. Bepaling inzake alternatieve geschillenoplossing zoals arbitrage of mediation _____%
      4. Acceptatiecriteria inclusief deliverables en installatie _____%
      5. Een overmachtsclausule _____%
      6. Een overzicht van de taken en verantwoordelijkheden van alle partijen _____%
      7. Een beperking van de aansprakelijkheid inzake het verlies, diefstal of onrechtmatige verwerking van vertrouwelijke informatie of gevoelige persoonsgegevens _____%
      8. Bepalingen inzake de verplichting om betrokkenen of organisaties te informeren na een inbreuk op de beveiliging van vertrouwelijke informatie en persoonsgegevens_____%

6. Heeft u een formele procedure voor het documenteren van wijzigingen in contracten gedurende de contractperiode? ☐ Ja ☐ Nee
7. Zijn er contracten voor ICT-projecten die uw opdrachtgever eerder met een andere partij heeft beëindigd? ☐ Ja ☐ Nee
8. Hoeveel procent van uw omzet besteedt u uit aan onderaannemers? _____%
9. Vereist u van uw onderaannemers dat zij een Beroepsaansprakelijkheidsverzekering hebben? ☐ Ja ☐ Nee
10. Heeft u volledige verhaalsrechten op uw onderaannemers? ☐ Ja ☐ Nee

11. Wat zijn de waarschijnlijke gevolgen in geval van een vertraging, gebrek e.d., van uw diensten of producten?

Meerdere opties zijn mogelijk:

☐ Dood of lichamelijk letsel

☐ Beschadiging, vernietiging of verlies van zaken

☐ Zeer geringe schade

☐ Onmiddellijke en omvangrijke financiële schade

☐ Omvangrijke cumulatieve financiële schade

Graag nadere informatie over de geselecteerde mogelijkheden

VIII Kwaliteitscontroles

1. Heeft u een formele procedure voor het documenteren van problemen, downtime en het reageren op klachten van opdrachtgevers? ☐ Ja ☐ Nee
2. Heeft u een schriftelijke en geformaliseerde procedure inzake kwaliteitscontrole? ☐ Ja ☐ Nee
3. Bewaart u bestanden en backups van uw contracten en kwaliteitscontroles? ☐ Ja ☐ Nee
4. Welke industriestandaarden hanteert u?

IX Intellectueel Eigendom (alleen in te vullen indien dekking hiervoor is gewenst)

1. Heeft u een formele procedure om te voorkomen dat u inbreuk maakt op het intellectueel eigendom van een derde? ☐ Ja ☐ Nee
2. Welk percentage van uw omzet bestaat uit uw producten of diensten:

die minder dan 3 jaar oud zijn _____%

die tussen de 3 en 5 jaar jaar oud zijn _____%

die ouder zijn dan 5 jaar _____%

X Data Privacy

1. Voor hoeveel dossiers met persoonsgegevens bent u verantwoordelijk? _____
2. Voor hoeveel dossiers met gevoelige data bent u verantwoordelijk? _____
3. Verwerkt, bewerkt of beheert u gegevens voor of namens een derde? ☐ Ja ☐ Nee
   a. Indien ja, Gelieve toe te lichten:

Indien ja,

   b. Voor hoeveel dossiers met persoonsgegevens die u voor of namens een derde verwerkt, bewerkt of beheert bent u verantwoordelijk? _____
   c. Voor hoeveel dossiers met gevoelige data die u voor of namens een derde verwerkt, bewerkt of beheert bent u verantwoordelijk? _____
4. Wordt betaalkaartinformatie verwerkt, verzameld, beheerd of bewerkt ☐ Ja ☐ Nee
   a. Indien ja, worden deze activiteiten uitbesteed?

b. Beschrijf het niveau van uw (of uw outsourcer/uitbesteder) PCI DSS compliance, het aantal transacties, aantal betaalkaarten waarvan u informatie heeft, de naam van de betalingsverwerker en of de betalingsverwerker u schadeloos stelt in geval van schade:

☐ Niveau 1 (meer dan 6M) ☐ Niveau 2 (1M tot 6M)

☐ Niveau 3 (20.000 tot 1M) ☐ Niveau 4 (minder dan 20.000)

XI Data en informatiebeveiliging

1. Welke van de volgende maatregelen heeft u (of uw provider, indien uitbesteed) geïmplementeerd ter bescherming van informatie en systemen tegen een datalek of cyberincident?

Beleid		Bescherming en Technologie		Bedrijfscontinuatie	
Functionaris gegevensbescherming	☐	Firewalls & Antivirus	☐	Bedrijfscontinuiteitsplan	☐
				Testen bedrijfscontinuiteitsplan:	
				Regelmatig	☐
				Niet regelmatig	☐
Medewerker verantwoordelijk voor de IT beveiliging	☐	Kwetsbaarheidsscan	☐	Crisis herstelplan	☐
				Testen crisis herstelplan:	
				Regelmatig	☐
				Niet regelmatig	☐
Privacy beleid goedgekeurd en geïmplementeerd	☐	Endpoint protection	☐	Systeemback-up:	
				Dagelijks	☐
				Wekelijks	☐
				Maandelijks	☐
Regelmatig trainingen op het gebied van privacy en cyber	☐	Indringer detectie systeem	☐	Back-ups zijn in een offline omgeving opgeslagen en zijn niet verbonden met het netwerk	☐
Maatregelen genomen om te (blijven) voldoen aan toepasselijke privacywetgeving, waaronder de AVG	☐	Encryptie van gevoelige data:		Duplicatie en redundantie van kritieke systemen in een offline omgeving	☐
		Volledig	☐		
		Gedeeltelijk	☐		
		Niet	☐		
Incident respons plan:	☐	Multi-factor authentication 2FA	☐	Duplicatie en redundantie van systemen	☐
Testen incident respons plan:				Duplicatie en redundantie van kritieke systemen in een offline omgeving	☐
Regelmatig	☐				
Niet regelmatig	☐				
Kritische updates en patches worden binnen één maand doorgevoerd	☐	Jaarlijks een externe pentest	☐		
Gebruik van Threat Intelligence	☐				
Authorisatiebeheer voor systemen	☐				
Testen van back-ups	☐				
Overige: (gelieve te omschrijven)					

XII Systemen

1. Noodzaak van informatiesystemen – Van welke systemen bent u het meest afhankelijk (inclusief uitbestede IT-diensten) en de gevolgen die het niet beschikbaar zijn voor elk van hen heeft.

Naam IT dienstverlener (noteer 'intern' als deze niet is uitbesteed)	Activiteiten, zoals data opslag, netwerk infra-structuur, PaaS,SaaS, back-ups, ERP,beveiliging.	Hersteltermijn (Recovery time objective)	Geschatte bedrijfsschade
		In uren	Per uur
			€
			€
			€
			€
			€

2. Voert u beoordelingen, assessments of audits uit om ervoor te zorgen dat IT-dienstverleners voldoen aan de beveiligingsvereisten van uw bedrijf? ☐ Ja ☐ Nee
3. Neemt u afstand van uw verhaalsrecht tegen één van de hierboven genoemde aanbieders in geval van onderbreking/tekortkoming van de dienstverlening? ☐ Ja ☐ Nee

XIII Media

1. Verkrijgt u schriftelijke toestemming of vrijwaring van externe content providers, waaronder freelancers, of andere belanghebbenden voor publicatie? ☐ Ja ☐ Nee
2. Onderhoud u forums of social media? ☐ Ja ☐ Nee
3. Heeft u een geschillenbeslechtings- en/of klachtenprocedure? ☐ Ja ☐ Nee
4. Gemiddels aantal unieke bezoekers van uw websites per maand: _____

XIV Netwerkbeveiliging

1. Zijn uw opdrachtgevers afhankelijk van netwerken en/of netwerkdiensten welke u aanbiedt? ☐ Ja ☐ Nee

   Indien ja:

   a. Zijn kritische en niet kritische netwerken gescheiden van elkaar ☐ Ja ☐ Nee
   b. Wordt netwerk activiteit proactief gemonitord ☐ Ja ☐ Nee

XV Schadeverloop

1. Bent u de laatste vijf jaar voor een schade aansprakelijk gesteld ? ☐ Ja ☐ Nee

   Zo ja, graag een volledige omschrijving van de aanspraak zoals datum, aard en (potentiële)financiële omvang van de aanspraak en welke maatregelen u heeft getroffen om de schade te beperken of herhaling te voorkomen.

2. Heeft er zich bij u de laatste vijf jaar ooit een cyberincident voorgedaan zoals hacking, malware, Ddos aanval, afpersing, programmeer- of menselijke fout? ☐ Ja ☐ Nee

   Zo ja, graag een volledige omschrijving van het incident zoals datum, aard en omvang van het incident en welke maatregelen u heeft getroffen om de schade te beperken of herhaling te voorkomen.

3. Bent u zich bewust van enig handelen of nalaten of zijn er omstandigheden die mogelijk tot een aanspraak of een cyberincident zoals hacking, malware, Ddos aanval, afpersing, programmeer- of menselijke fout kunnen leiden? ☐ Ja ☐ Nee

   Zo ja, graag een volledige omschrijving.

XVI Aanvullende informatie

Indien gewenst kunt u met betrekking tot uw antwoorden hieronder aanvullende informatie toevoegen

XVII COVID-19

1. Op welke wijze heeft COVID-19 uw activiteiten beïnvloed?

2. Voorziet u potentiële claims met betrekking tot COVID-19? ☐ Ja ☐ Nee

   (Bijvoorbeeld als gevolg van vertraging bij projecten) Zo ja, gaarne toelichten.

3. Wat zijn de implicaties van het niet kunnen werken op het terrein van de opdrachtgever (indien van toepassing)?

Ondertekening

Ondergetekende, bevoegd om voor de onderneming te tekenen, verklaart de bovenstaande vragen volledig en naar waarheid te hebben beantwoord en geen voor deze verzekering belangrijke aspecten te hebben verzwegen en/of niet geheel juist te hebben voorgesteld.

Ter informatie: in afwijking van het bepaalde in artikel 7:928 e.v. BW, is Chubb ontslagen van iedere uitkeringsplicht indien blijkt dat verzekeringnemer bij het aanvragen van de verzekering onjuiste of onvolledige informatie heeft verstrekt en Chubb de verzekering niet of niet onder dezelfde voorwaarden zou hebben gesloten, indien Chubb de juiste feiten gekend had. Verzekeringnemer verklaart zich hiermee akkoord.

Plaats _____ Datum _____

Naam _____ Functie _____

Handtekening

S.v.p. meezenden:
- Kopie van uw standaard contract(en), incl. algemene voorwaarden, en evt. SLA en/of verwerkersovereenkomst
- Kopie contract(en), incl. algemene voorwaarden van uw toeleverancier(s), onderaannemer(s), hosting provider e.d.

Begrippenlijst

Autorisatiebeheer voor Systemen - Access Management Controls omvat het management van gebruiksnamen, wachtwoorden en toegang tot systemen en informatie.

Cyber-incident- Cyber-incident betekent ongeautoriseerde toegang tot computer systemen, hacking, malware, virus, cyber afpersing, distributed denial of service-aanval, misbruik door voorkennis, menselijke fout of programmeerfout of een andere aan cyber gerelateerde gebeurtenis.

Datalek- Een datalek betekent date er een incident heeft plaatsgevonden waarbij gevoelige persoonsgegevens of bedrijfsgevoelige informatie is gestolen, kwijtgeraakt of bekeken bij of door een onbevoegde partij.

Encryptie – Encryptie is een methode om data vanuit een leesbare format te converteren naar een gecodeerde format. Het kan alleen weer leesbaar worden (worden geopend) met behulp van een sleutel.

Endpoint Protection – Endpoint Protection zorgt voor de bescherming en bewaking van de eindpunten in uw netwerk. Eindpunten omvatten desktop-en laptopcomputers, tablets, mobiele telefoons, servers en elk ander apparaat dat verbonden is met uw netwerk.

Gevoelige data– Onder gevoelige data wordt o.a. verstaan gezondheids-of medische dossiers van werknemers of klanten, door de overheid uitgegeven identificatienummers, gebruikersnamen en wachtwoorden, e-mailadressen, creditcardnummers, intellectueel eigendom of andere persoonlijk identificeerbare informatie.

Indringer Detectie Systeem – Is een apparaat of software dat een network monitort op kwaadwillige activiteiten of beleidsschendingen.

Media-aansprakelijkheid – Media-aansprakelijkheid omvat ieder claim voor het kleineren, smaad, laster in handelsbetrekkingen, schijnvertoning, plagiaat of iets dergelijks van uw website of social media accounts.

PCI DSS -Payment Card Industry Data Security Standard. Dit is een standaard voor gegevensbescherming voor kaartaccepterende bedrijven. Een standaard voor gegevensbescherming van betaalkaartinformatie. De gevoelige betaalkaartinformatie die moet worden beschermd is het kaartnummer, de vervaldatum, de CVC-code en de naam van de kaarthouder.

Recovery Time Objective - De beoogde tijdsduur waarbinnen het bedrijfsproces moet worden hersteld na een storing of verstoring om onaanvaardbare gevolgen te vermijden die samenhangen met een onderbreking van de bedrijfscontinuïteit.

Threat Intelligence– Bedreigingsinformatie is informatie over huidige beveiligingsbedreigingen, kwetsbaarheden, doelen, slechte actoren en implicaties die kunnen worden gebruikt om beveiligingsbeslissingen.