# Aanvraagformulier Cyber verzekering

Aanvraag offerte

Aanvraag nieuwe verzekering

Wijziging bestaande verzekering onder polisnummer

## GEGEVENS VERZEKERDE

|  |  |
| --- | --- |
| Naam |  |
| Adres |  |
| Website |  |

## FINANCIËLE GEGEVENS

|  |  |  |  |
| --- | --- | --- | --- |
|  | In het laatste complete financiële jaar | Huidig jaar (bij benadering) | Volgend jaar (als ingeschat ) |
| Jaarlijkse inkomsten |  |  |  |
| Hoeveel procent van het jaarlijks budget wordt gespendeerd aan IT? |  | | |
| Huidig aantal werknemers |  | | |

## CLAIMS GESCHIEDENIS

|  |
| --- |
| Is er in de afgelopen 5 jaar sprake geweest van een binnentreding in het computersysteem, cybervirusincident, een aanval middels kwaadwillige code, verlies van computer, verlies van draagbare media, een hack incident, pogingen tot afpersing via de computer of daarmee vergelijkbare gebeurtenissen?  (Zo ja dan ontvangen wij graag een nadere omschrijving met details van deze gebeurtenis) |
| Heeft u in de afgelopen 5 jaar claims of klachten ontvangen aangaande een privacy-schending, identiteitsdiefstal, diefstal van informatie, inbreuk op intellectueel eigendom of bent u verplicht geweest personen te informeren vanwege een privacy schending?  (Zo ja dan ontvangen wij graag een nadere omschrijving met details van deze gebeurtenis) |
| Bent u de afgelopen 5 jaar onderwerp van justitieel onderzoek geweest met betrekking tot een schending van privacywetgeving of andere aanverwante regelgeving zoals de Wet Datalekken?  (Zo ja dan ontvangen wij graag een nadere omschrijving met details van deze gebeurtenis) |
| Indien sprake is geweest van één van bovengenoemde gebeurtenissen vernemen wij graag hoe deze incidenten uiteindelijk zijn opgelost |

## DATA BEOORDELING

|  |  |  |  |
| --- | --- | --- | --- |
| Geef hieronder aan welke data de gemeente elektronisch in bewaring heeft en bij benadering de aantallen van die data | | | |
| Persoonsgegevens |  | Rijbewijsnummers |  |
| Burger servicenummers |  | Medische informatie |  |
| Credit Card Informatie: |  | Financiële informatie |  |
| Persoonlijke Informatie ten aanzien van bv. religieuze voorkeuren e.d. |  | Anders: |  |

## WERKNEMERS

|  |  |  |
| --- | --- | --- |
| Heeft de gemeente een privacy-officier aangesteld of iemand die de leiding heeft over beveiliging van informatie? | Ja | Nee |
| Wordt de achtergrond van IT-medewerkers, bij aanstelling, onderzocht middels opvraag van een VOG-verklaring? | Ja | Nee |
| Wordt de gebruikerstoegang van medewerkers gebaseerd op de functie en jaarlijks gecontroleerd op geschiktheid? | Ja | Nee |
| Worden alle gebruikers van het netwerk verplicht om op zijn minst elk kwartaal hun wachtwoorden te wijzigen. En worden ze daarbij geïnstrueerd om tenminste zes karakters te gebruiken met een combinatie van hoofdletters, cijfers en symbolen? | Ja | Nee |
| Is de toegang tot het netwerk onmiddellijk beëindigd nadat men al dan niet zelf de verbinding heeft verbroken ? | Ja | Nee |

## NETWERK BEOORDELING

|  |  |  |
| --- | --- | --- |
| Is uw netwerk extern beoordeeld en/of getest op veiligheid in het afgelopen jaar? | Ja | Nee |
| Zijn alle kritische aanbevelingen opgevolgd? | Ja | Nee |

## FYSIEKE VEILIGHEID

|  |  |  |
| --- | --- | --- |
| Wordt een clean desk beleid gevolgd op de werkplekken? | Ja | Nee |
| Heeft u een databehoud- en vernietigingsbeleid in geval van cybercrime? | Ja | Nee |

## SYSTEEMBEVEILIGING

|  |  |  |
| --- | --- | --- |
| Zijn er firewalls op alle externe verbindingspunten? | Ja | Nee |
| Wordt antivirus software gedraaid op het netwerk, inclusief al het inkomend verkeer? | Ja | Nee |
| Binnen welke termijn worden belangrijke patches geïmplementeerd? | 24 uur  72 uur  Week  anders |  |
| Heeft u antivirus software en firewalls op alle: |  |  |
| 1. Werkstations 2. Laptops | Ja  Ja | Nee  Nee |
| Wat is bij benadering het aantal servers op uw netwerk? |  | |
| Op hoeveel locaties zijn servers aanwezig? |  | |

## BELANGRIJKE SYSTEEMGEGEVENS

|  |  |  |
| --- | --- | --- |
| Zijn belangrijke systeem gegevens gescheiden van elkaar (hiërarchisch) in een geïsoleerde omgeving? | Ja | Nee |
| Zijn de belangrijke systeem gegevens geëncrypteerd? | Ja | Nee |

## REMOTE ACCESS

|  |  |  |
| --- | --- | --- |
| Is toegang op afstand op het netwerk van de gemeente toegestaan? | Ja | Nee |
| Zo ja, is toegang dan enkel toegestaan middels zogenoemde tweetrapsauthenticatie? | Ja | Nee |
| Zijn alle externe toestellen die verbinding maken verplicht om antivirussoftware of een firewall te installeren, die in overeenstemming is met het beleid van de gemeente ten aanzien van updates en patches? | Ja | Nee |

## DRAGERS VAN DATA

|  |  |  |
| --- | --- | --- |
| Worden alle gevoelige gegevens die fysiek buiten gemeente terrein gaan, zoals via laptop, mobiele telefoon of ander draagbaar toestel zoals een usb-stick geëncrypteerd? | Ja | Nee |
| Indien niet, bewaart u gevoelige data op bovengenoemde toestellen? | Ja | Nee |
| Beschikt u over processen of beleid die in werking worden gezet indien een toestel als bovengenoemd wordt verloren of gestolen? | Ja | Nee |
| Worden gevoelige gegevens geëncrypteerd wanneer ze buiten uw netwerk naar anderen worden verzonden? | Ja | Nee |

## RISICOMANAGEMENT PROCEDURE

|  |  |  |
| --- | --- | --- |
| Zijn er procedures ten aanzien van Risicomanagement? | Ja | Nee |
| Worden logboeken bijgehouden van veranderingen in het informatiesysteem? | Ja | Nee |
| Zijn er maatregelen om dataclassificatie mogelijk te maken voorhanden? | Ja | Nee |
| Is er een calamiteitenplan dat ziet op beveiligingsinbreuken en dataverlies? | Ja | Nee |
| Zijn de rollen in deze plannen duidelijk en zijn vervangende medewerkers aangewezen voor elke sleutelrol, zodat er altijd een reserve is? | Ja | Nee |
| Is het calamiteitenplan en beleid op het punt van cyberveiligheid gebaseerd op een externe bron? | Ja | Nee |
| Zo ja welke? |  |  |

## UITBESTEDE WERKZAAMHEDEN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Geef hieronder alle voor deze verzekering van belang zijnde bedrijven weer en de dienst die zij verlenen | | | | |
| Managed Security Services: |  |  |  | |
| Cloud / Back-up / Website Hosting: |  |  |  | |
| Internet Service Providers: |  |  |  | |
| Business Critical Software Providers: |  |  |  | |
| Data Processors: |  |  |  | |
| POS Hardware Providers: |  |  |  | |
| Co-location Services: |  |  |  | |
| Worden bovengenoemde bedrijven gecontroleerd om te bezien of ze voldoen aan de veiligheidsstandaard van de gemeente? | | | Ja | Nee |
| Zo niet wat voor due diligence procedure wordt dan uitgevoerd? | | |  | |

## REGELGEVING

|  |  |  |
| --- | --- | --- |
| Heeft de gemeente een privacy beleid? | Ja | Nee |
| Staat dit beleid op de gemeentelijke website? | Ja | Nee |

## DATA RECOVERY EN BEDRIJFSSCHADE

|  |  |  |
| --- | --- | --- |
| Is er een geschreven Calamiteitenplan dat tevens ziet op een onderbreking-uitval van het netwerk of computersystem van de gemeente? | Ja | Nee |
| Wordt dit plan jaarlijks getest? | Ja | Nee |
| Worden alle aanbevelingen die uit de test voortvloeien opgevolgd | Ja | Nee |
| Welke termijn is nodig om de belangrijke essentiële systemen volledig te herstellen | Minder dan 6 uur  6-10 uur  10-12 uur  12-24 uur  Anders |  |
| Welke termijn is nodig om de minder belangrijke of essentiële systemen te herstellen? | Minder dan 6 uur  6-10 uur  10-12 uur  12-24 uur  Anders |  |
| Bestaat de mogelijkheid om over te schakelen naar een hot site in het geval de hosting site plat wordt gelegd? | Ja | Nee |
| Zo niet wat doet u dan? |  | |
| Worden er fysieke back-ups gemaakt die off-site worden opgeslagen? | Ja | Nee |
| Hoe vaak worden deze back-ups gemaakt? | Dagelijks  Wekelijks  Tweewekelijks  Maandelijks  Anders |  |
| Hoe lang worden back-ups bewaard? |  | |

## CREDIT CARD DATA

|  |  |  |
| --- | --- | --- |
| Behandelt of verwerkt u betalingen via bank of credit card? | Ja | Nee |
| Hoeveel transacties per jaar verwerkt of behandelt u? |  | |
| Voldoet u aan de huidige Payment Card Industry Data Security Standard?  (Voor meer informatie zie: <https://www.pcicomplianceguide.org/pci-faqs-2/> of <http://www.paysquare.eu/nl/nl/ondernemers/meerinformatie/veiligomgaanmetkaartgegevens/veelgestelde-vragen-over-pci-dss.jsp>) | Ja | Nee |

## MULTIMEDIA

|  |  |  |
| --- | --- | --- |
| Heeft de gemeente een protocol om alle content te controleren voordat deze wordt geplaatst op een website of op Social Media, die gemaakt en onderhouden wordt door of voor de gemeente? | Ja | Nee |

**Het is mogelijk dat er naar aanleiding van antwoorden op boven gestelde vragen nog aanvullende vragen worden gesteld c.q. inspectie wordt verricht.**

## VERKLARING

De aanvrager verklaart mede gelet op de inhoud van artikel 7:928 BW, dat de gegeven informatie/ verklaringen juist en volledig is/zijn en dat mededeling is gedaan (na gedegen onderzoek) van de feiten en omstandigheden die voor Verzekeraar van belang zijn voor de beoordeling van zowel het te verzekeren risico als ten aanzien van de verzekeringnemer en verzekerden.  
De verklaringen vormen, tezamen met de overige aan Verzekeraar verstrekte informatie in dit formulier, de grondslag voor- en een integraal onderdeel van- de verzekeringsovereenkomst.   
Aanvrager verplicht zich voorts om verzekeraar onverwijld schriftelijk te informeren indien de gepresenteerde feiten zijn gewijzigd voordat deze verzekeringsovereenkomst is afgesloten.

Handtekening

Functie

Datum