|  |
| --- |
| **Cyber Risk Insurance Detailed Application** |
|  |
| **NOTES** | **All questions must be completed** |
|  | **Each policy is provided on a claims-made and reported basis. Defence expenses are included within the limits of coverage.** **Name of Applicant: Any other entity directly or indirectly through ownership, control or otherwise (including subsidiaries) and the relationship to the Name of the Applicant must be declared. A separate application for each entity declared may be required.**  |
|  |
| **General Information** |
| Legal Name of Applicant |       |
| Key Contact |       | Position |       |
| Key Contact Email Address |       |
| Mailing Address |       | Postal code |       |
| Phone |       | Email |       |
| Website Address |       |  |  |
| Key Broker Contact |       |
| Brokerage Name |       |
| Brokerage Address |       | Postal code |       |
| Phone |       | Email |       |
|  |
| **Operations** |
| Applicant is | Sole Proprietor |       | Partnership |       |  | Corporation |       |
|  | Municipality |       | Other (Explain) |        |
|  |
| Please describe the Applicant’s operations and services |
|       |
| Date established (dd/mm/yyyy) |       |
| Indicate all Countries outside of Canada that the Applicant operates in |
|       |
|  |

|  |
| --- |
| **If operating in Countries outside of Canada, indicate percentages of revenue anticipated in the current year** |
| Canadian |       | **%** | U.S. |       | **%** | Other  |       |       | **%** |
| If 'Other' is selected indicate the Country and Percentage.  |

|  |
| --- |
|  |
| **Total Domestic Gross Revenues**  |
| Prior Year – Gross | $ |       | Last Year Gross Profit | $ |       |
| Please state which financial institution(s) you use for your commercial banking: |
|       |
|  |

|  |
| --- |
|  |
| **Claims, Circumstances and Other Historical Information** |
| Please tick all boxes below that relate to any cyber incident that you have experienced in the last three years (there is no need to highlight events that were successfully blocked by security measures): |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| [ ]  | Cyber Extortion | [ ]  | Data Loss | [ ]  | Denial of Service Attack | [ ]  | IP Infringement |
| [ ]  | Malware Infection | [ ]  | Privacy Breach | [ ]  | Ransomware | [ ]  | Theft of Funds |
| [ ]  | Other (please specify) |       |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| If you ticked any of the boxes above, did the incident(s) have a direct financial impact upon your business of more than $10,000 | YES |       | NO |       |
| **If ‘yes’ please provide more information below, including details of the financial impact and measures taken to prevent the incident from occurring again:** |
|       |
| Is the Applicant aware of any circumstances that could give rise to a claim under this insurance policy? | YES |       | NO |       |
| **If ‘yes’ please explain the circumstances and/or potential claims:** |
|       |
| Within the last 3 years have you been subject to any complaints concerning the content of your website, advertising materials, social media, or other publication? | YES |       | NO |       |
| **If ‘yes’ please explain the circumstances:** |
|       |
|  |
| **Revenue Analysis** |
| If applicable, please provide the following details for your top 5 clients |
| **Name of Client:** | **Primary Services:** | **Annual revenue derived from client:** |
|       |       | $       |
|       |       | $       |
|       |       | $       |
|       |       | $       |
|       |       | $       |
|  |
| **IT Infrastructure and Resourcing**  |
| Please confirm the name of your managed service provider (if applicable) |       |
| What is the approximate number of servers on your network? |       |
| Please describe any on premises servers that are exposed to the internet? |       |
| Please list the IP addresses on which any on-premises servers or other IT infrastructure are hosted: |
|       |
| What is the approximate number of desktops and laptops on your network? |       |
| What is your annual IT budget? |       |
| What approximate percentage of your IT budget is spent on IT security? |       |
|  |
| Does your network have segmentation between: |
| Geographic Locations? | YES |       | NO |       |
| Business units? | YES |       | NO |       |
| Databases for PII/PHI/PCI? | YES |       | NO |       |
| End of life/unsupported software and rest of network? | YES |       | NO |       |
| Is any part of our IT infrastructure outsourced to third party technology providers, including application service providers? | YES |       | NO |       |
| If you answered ‘yes’ to the question above, please list your critical third-party technology providers below (up to a maximum of 10), including a brief summary of the technology services they provide you: |
|       |
| **Data Storage and Management**  |
| **Please provide the approximate number of unique individuals that you collect, store and/or process personally identifiable information from whether on your own systems or with third parties:** |
|  |
| **Data Type** | **Number (or Approximate) of Unique Individuals** |
| Sensitive Data (e.g., medical records, passport details, social security numbers) |       |
| Non-Sensitive Data (e.g., full names, addresses, email addresses etc.) |       |
|  |
| Do you collect, process, store, transmit or have access to any Payment Card Information (PCI)? | YES |       | NO |       |
| If ‘yes’, what is the estimated annual volume of payment card transactions (credit cards, debit cards, etc.)? |       |
|  |
| Please describe your approach towards protecting sensitive and confidential information (e.g., access controls, encryption, network segmentation etc.): |
|       |
| Do you implement encryption on laptop computer, desktop computers and other portable media devices? | YES |       | NO |       |
| Please provide details of how often you purge records that are no longer required: |
|       |
| Please provide details on how you store your back-ups of critical data (e.g., online back-ups stored on your organizations live environment, offline back-ups stored on a removable storage device that is fully disconnected and inaccessible from the live environment, back-ups stored with an online cloud storage provider etc.): |
|       |
| Please provide details on the frequency of your back-ups, including the frequency of full system back-ups and the frequency of incremental/differential back-ups of critical data: |
|       |
| Please provide details on how you secure your back-ups (e.g., back-ups are disconnected and inaccessible from the live environment, multi-factored authentication is required to access cloud back-ups etc.) |
|       |
| Please provide details on how you test your back-ups, including details on how frequently you test the full restoration of key server configurations and data from back-ups: |
|       |
| Please provide details on the number of back-up copies you take, including details on how you prevent separate back-up copies being impacted by the same event (if applicable): |
|       |
|  |
| **Endpoint Security** |
|  |
| Which endpoint protection product do you use on your network?Please provide the name of the vendor and product used |       |
| Do you use an endpoint detection and response (EDR) product on your network? | YES |       | NO |       |
| If ‘yes’, what product do you use? |       |
|  |  |  |
| Please provide an overview of how your EDR product is monitored and managed (e.g., internal IT team or outsourced to a third party): |
|       |
| Is the EDR product deployed on all endpoints on your network? | YES |       | NO |       |
| If ‘no’, what percentage of endpoints do not have EDR deployed and why is it not deployed on these endpoints: |
|       |
| Do you have any endpoint management software exposed to the internet (Kaseya, etc.)? | YES |       | NO |       |
| If so, what security controls do you have around that? |
|       |
| Do you have secure/hardened baseline configuration which is regularly reviewed and updated by an information security professional? | YES |       | NO |       |
| If ‘yes’ to the above, is this baseline configuration materially rolled out across servers, laptops, desktops, and managed mobile devices? | YES |       | NO |       |
|  |
| **Perimeter Security** |
| Do you have next-generation firewalls deployed at all network ingress/egress points? | YES |       | NO |       |
| Do you have inbound and outbound firewall configuration with log retention? | YES |       | NO |       |
| If ‘yes’, for how long are these firewall logs retained? |       |
| How often do you conduct vulnerability scanning of your network perimeter? |       |
| How often do you conduct penetration testing of your network architecture? |       |
| Please provide details of the third-party providers you use to conduct penetration testing (if applicable) |       |
| Please confirm whether multifactor authentication is required for all remote access to your network? | YES |       | NO |       |
| If you use an alternative method for securing remote access to your network, such as certificate-based authentication for devices, please provide details here: |
|       |
| Please confirm whether multifactor authentication is required to access all cloud resources holding sensitive or confidential information | YES |       | NO |       |
| Please confirm if multifactor authentication is enforced on all Virtual Private Network (VPN), Remote Desktop Protocol (RDP), RDWeb, RD Gateway, or other remote access | YES |       | NO |       |
|  |
| **Business Continuity**  |
| Do you have a business continuity/disaster recovery plan? | YES |       | NO |       |
| If ‘yes’, how frequently is it tested? |       |
| Based on testing, what is your proven recovery time objective for critical systems to restore operations after a cyber attack or other unplanned outage? |       |
| Can backups be accessed via an authentication mechanism outside of Active Directory? | YES |       | NO |       |
|  |
| **Email Security** |
| Please confirm that multifactor authentication is enabled for remote access to all company email accounts | YES |       | NO |       |
| Do you simulate phishing attacks to test employees at least annually? | YES |       | NO |       |
| Do you use email filtering software to scan all inbound and outbound email messages in order to filter out spam and malicious content? | YES |       | NO |       |
| If you answered ‘yes’ to the previous question, please state the name of the vendor and product used for email filtering |       |
| Do you use Microsoft Office 365? | YES |       | NO |       |
| If yes, do you use: |  |  |  |  |
| Microsoft Sentinel (free or paid tier)? | YES |       | NO |       |
| Advance Threat Protection (ATP) add-on? | YES |       | NO |       |
| Other email security products? | YES |       | NO |       |
| If so, what products? |       |
| If you are an Office 365 user, please provide your Microsoft Secure Score (administrators can find the score using the following link <https://security.microsoft.com/securescore>): |       |
| Do you use self-hosted Microsoft Exchange servers? | YES |       | NO |       |
| If ‘yes’, have you disabled on premises Exchange Web Services? | YES |       | NO |       |
| What other email security controls do you have in place to mitigate risk (Anti-Malware, Anti-phishing, other)? Please provide details and context. |
|       |
|  |  |  |  |  |
| **Network Security**  |
|   |
| Please provide details on how you protect privileged user accounts (e.g., using privileged access management solutions, restricting privileged user accounts to specific devices, enhanced monitoring of accounts for anomalous usage, multifactor authentication enabled for remote access etc.): |       |
| Do non-IT users have local administrator rights on their laptops/desktops? | YES |       | NO |       |
| What controls are in place to prevent privilege escalation? |
|       |
| Do you use a network monitoring solution to alert your organization to suspicious activity or malicious behaviour on your network? | YES |       | NO |       |
| If you answered ‘yes’ to the previous question, please state the name of the vendor and product used for network monitoring: |       |
| Please provide details on whether you have a Security Operations Centre (SOC) that is responsible for event monitoring and detection, vulnerability management and incident response. Please include details on the hours of operation and whether this is an internal function or outsourced to a third party: |
|       |
| Do you have any end of life or end of support software? | YES |       | NO |       |
| If ‘yes’, please provide details on what the end of life or end of support software is, how it is used, whether it is segregated from the rest of the network and if so, how it is segregated: |
|       |
| Please describe your patch management process and how you ensure that all critical patches are applied in a timely fashion, including a timeframe of how quickly you would implement patches for zero-day vulnerabilities after they have been released by the vendor: |
|       |
| Please provide details of any major changes that you have planned for your IT infrastructure in the next 12 months (if any): |
|       |
| **Additional Controls**  |
| Please confirm that before any change is made to a third party’s account details, you obtain authorization from the third party via an authentication method which is different to the original method used to request the change? | YES |       | NO |       |
| Please confirm that before you transfer funds to an account that you haven’t paid into before, you obtain authorization from the recipient of the funds via an authentication method which is different to the original method used to request the transfer? | YES |       | NO |       |
| Do you provide training on phishing/social engineering scams for all employees involved in transferring funds on behalf of your organization on at least an annual basis? | YES |       | NO |       |
| Do you enforce procedures to remove content (including third party content) that may infringe or violate any intellectual property or privacy right? | YES |       | NO |       |
|  |  |  |  |  |
| Please tick all the boxes below that relate to the controls that you currently have implemented within your IT infrastructure (including where provided by a third party).  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| [ ]  | Application Whitelisting | [ ]  | Asset Inventory | [ ]  | Custom Threat Intelligence | [ ]  | Database Encryption |
| [ ]  | Data Loss Prevention | [ ]  | DDoS Mitigation | [ ]  | DMARC | [ ]  | DNS Filtering |
| [ ]  | Employee Awareness Training | [ ]  | Incident Response Plan | [ ]  | Intrusion Detection System | [ ]  | Perimeter Firewalls |
| [ ]  | Security Info & Event Management | [ ]  | Virtual Private Network (VPN | [ ]  | Web Application Firewall | [ ]  | Web Content Filtering |

|  |
| --- |
| Please provide the name of the software or service provider that you use for each of the controls highlighted above: |
|       |
|  |
| **Cyber Crime** |
|  | Please estimate the number of fund transfers sent on a daily basis: |       |
|  | Estimate the average size of a fund transfer |       |
|  | Please confirm dual verification is in place before amending account details and sending fund transfer requests? (for example, by phone and email) | YES |       | NO |       |
|  | For fund transfers of $25k, is authorization from more than one individual required? | YES |       | NO |       |
|  | Are all employees with fund transfer authority given specific cybercrime training? | YES |       | NO |       |
|  | Are external emails flagged to notify the employee it has come from the outside network?  | YES |       | NO |       |
|  |

|  |
| --- |
| **Please Read** |
| The Applicant hereby represents after inquiry, that information contained herein and in any supplemental applications |
| or forms required hereby, is true, accurate and complete, and that no material facts have been suppressed or |
| misstated. The Applicant acknowledges a continuing obligation to report to the Company as soon as practicable any  |
| material changes in all such information, after signing the application and prior to issuance of the policy, and  |
| acknowledges that the Company shall have the right to withdraw or modify any outstanding quotations and/or |
| authorization or agreement to bind the insurance based upon such changes. |
|  |
| Further, the Applicant understands and acknowledges that: |
| 1.  | If a policy is issued, the Company will have relied upon, as representations, this application, any supplemental |
|  | applications, and any other statements furnished to the Company in conjunction with this application, all of  |
|  | which are hereby incorporated by reference into this application and made a part thereof. |
|  |
| 2. | This application will be the basis of the policy and will be incorporated by references into and made part of  |
|  | such policy; and |
|  |
| 3. | The Applicant's failure to report to its current insurance company any claim made against it during the current  |
|  | policy term, or act, omission or circumstances which the Applicant is aware of which may give rise to a claim  |
|  | before the expiration of the current policy may create a lack of coverage for each Applicant who had a basis to  |
|  | believe that any such act, omission or circumstances might reasonably be expected to be the basis of a claim. |
|  |  |
| 4. | The policy applied for provides coverage on a claims made and reported basis and will apply only to claims  |
|  | that are first made against the insured and reported in writing to the Company during the policy period.  |
|  | Claims expenses are within and reduce the limit of liability. |
|  |
| The Applicant hereby authorizes the release of claim information to the Company from any current or prior  |
| Insurer of the Applicant. |
|  |
| **Fraud Warnings** |
| Any person who knowingly includes any false or misleading information on an application for an insurance policy  |
| may be subject to criminal and civil penalties. |
|  |
| **Applicant Acknowledgement** |

|  |
| --- |
| The undersigned authorized officer of the organization declares that to the best of his/her knowledge, the statements |
| set forth herein are true. Signing of this application does not bind the Company (Insurer) to offer, nor the Applicant to  |
| accept insurance, but it is agreed that this form shall be the basis of the contract should a policy be issued, |
| and this form will be attached to and become part of the policy. |
|  |
| The undersigned, on behalf of the insured organization, acknowledges that any personal information provided in  |
| connection with this application (including but not limited to the information contained in this form) has been collected |
| in accordance with applicable privacy legislation and this information shall only be used or shared by Company to  |
| assess, underwrite and price insurance products and related services, administer and service insurance policies,  |
| evaluate and investigate claim, detect and prevent fraud, analyze and audit business results and/or comply with. |
| regulatory legal requirements |
| **Applicant Name** |       | **Title/Position** |       |
| **Applicant Signature** |       | **Date** |       |
| **Broker Name** |       |  |
| **Broker Signature** |  |  |