

# HSB TOTAL CYBER™ CYBER RISK INSURANCE APPLICATION

INSURANCE UNDERWRITTEN BY

**THE BOILER INSPECTION AND INSURANCE COMPANY OF CANADA, PART OF HSB GROUP**

This questionnaire is neither an offering nor binding of an insurance contract. Furthermore the completion of this questionnaire does not obligate the insurer to offer coverage to you. The answers to the questions are very important to us for assessing the risk in order to provide cyber insurance to you based on the information we receive. Therefore we rely on your statements made in the questionnaire which are the basis for the insurance contract.

Please complete the following details for the entire company or group (including all subsidiaries) that is applying for the insurance policy

## Company | Applicant Information

Business Name  Applicant Name

Business Description

### \*PRIMARY INDUSTRY

Please select the most appropriate industry class that applies to your organization

- Accommodation & Food Services
- Educational Services
- Mining, Quarrying, Oil & Gas Extraction
- Religious Organizations
- Wholesale
- Agriculture, Forestry, Fishing & Hunting
- Finance & Insurance
- Personal Services
- Rental & Leasing
- Arts, Entertainment & Recreation
- Healthcare & Social Assistance
- Professional Services
- Retail Trade
- Automotive Repair
- Information & Technology
- Public Administration
- Transportation & Warehousing
- Construction
- Manufacturing
- Real Estate
- Utilities

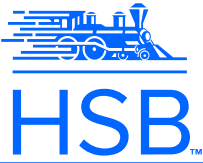
Business Address (Head Office) Unit No.  Street  City

City  Province  Postal Code

Mailing Address (if different from above) Unit No.  Street  City

City  Province  Postal Code

Business Website (URL)



Date Established  Number of Employees

Annual Gross Revenue  Annual Net Operating Expenses \*

Which of the following categories of sensitive data is your organization responsible for collecting, maintaining, processing or have access to? (Please select all that apply)

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Payment Card Information (PCI)

\*For any non-profit organizations, please use Annual Net Operating Expenses in lieu of Annual Gross Revenue

## Policy Details

Policy Period  Effective Date  to  Expiry Date

### Combined Annual Aggregate Limit Requested

- \$25,000  \$50,000  \$100,000
- \$250,000  \$500,000  \$1,000,000

### Deductible Requested \*

- \$1,000  \$2,500  \$5,000
- \$10,000  \$25,000  \$50,000
- \$100,000

\*Minimum deductible available for \$250,000, \$500,000 and \$1,000,000 limits is \$2,500

**Previous Cyber Insurance**

With respect to the prior insurance history, which of the following statements apply to your organization? (please select all that apply)

- You currently hold or have ever held cyber insurance providing the same or similar coverage as the insurance sought
- Any insurer cancelled or non-renewed a policy that provided the same or similar coverage as the insurance applying for

**Previous Cyber Incidents**

Have you, at any time during the past 36 months, experienced any cyber incident(s) mentioned below or experienced a lawsuit or other formal dispute (with either a private party or government agency) arising from a cyber incident?  YES  NO

\*If the above answer is YES, the following questions must be answered.

\*If the above answer is NO, please proceed to the next page

How many cyber incidents did you experience in the past 36 months?  1  2  3 or more

What was the total amount of loss from the cyber incident(s) in the past 36 months  Less than \$10,000  \$10,001 - \$50,000  \$50,001 - \$100,000  More than \$100,000

Please select any boxes below that relate to any cyber incident that you have experienced in the last 36 months:

- Business Income Loss
- Cyber Extortion
- Data Loss
- Denial of Service Attack
- Electronic Media Incident
- Fraud Loss
- Incident Response Costs
- Malware Infection & Hacking
- Network Service Failure Liability
- Personal Identity Theft
- Privacy Breach
- Ransomware
- Regulatory Proceeding
- Theft or Loss of Laptops
- Other (please specify: \_\_\_\_\_)

Are you aware of any actual or alleged fact, circumstance, situation, error or omission, or potential issue which might give rise to a loss or claim against you under the cyber insurance policy for which you are applying for or any similar insurance presently or previously in effect or currently proposed?  YES  NO

Please provide details regarding the above cyber incident(s), including dates of loss, Cause of Loss and individual loss amounts:

Please provide details regarding any and all corrective actions taken in response to above cyber incident(s) to mitigate future exposures:

**No additional information is needed if limit requested does not exceed \$50,000. Please go to Page 5. Below additional questions are required for \$100,000, 250,000, \$500,000 and \$1,000,000 Limits:**

**Backup and Archiving**

With respect to the data backup, which of the following statements apply to your organization? (please select all that apply)

Performing backups of business critical data on at least a weekly basis

The backups of business critical data is stored offsite in a secure location

You store backups of business critical data in an offsite secure location and you test the restore process

If you test your restore process, please select the frequency

Monthly

1 – 6 Months

6 months or more

**Computer Systems Control**

With respect to your computer/network systems, which of the following incident preventative actions do you currently have in place? (Please select all that apply)

Using up-to-date anti-virus and anti-malware protection on all your endpoints (desktops, laptops, servers, etc.) and firewalls on all of your internal access points

Implementing all critical patches for zero day vulnerabilities after they have been released by the vendor

Requiring Multi Factor Authentication (MFA) for any remote access to your network as well as all Company email accounts

Providing each user of your system with a separate individual account

**Internal Policies and Standards**

Which of the following data security and privacy policies have you implemented at your organization? (Please select all that apply)

Restricting employees' and external users' access to IT systems privileges and personal information on a business-need-to-know basis

Implementation of a Business continuity plan, recovery plan and/or an incident response plan

Encryption all of your mobile devices (laptops, flash drives, mobile phones, etc.) and confidential data?

Reviewing all advertising and other content prior to publication

Provide annual training and education to employees to increase security awareness and to prepare users to be more resilient and vigilant against phishing

Implementing a password policy enforcing the use of long and complex passwords across your organization?

Long and complex passwords are defined as: eight characters or more; not consisting of words included in dictionaries; free of consecutive identical, all-numeric or all-alphabetic characters.

## Declaration and Authorization

**BY PROVIDING MY E-SIGNATURE BELOW I CONFIRM THAT:**

- 1) If I accept payment (credit and debit) cards, I comply with Payment Card Industry Data Security Standards;
- 2) If I handle health information, I comply with the Personal Information Protection and Electronic Documents Act;
- 3) I have read and understood all of the questions in this Application for insurance and I understand that the answers I have provided will be relied upon by the Insurer in assessing my Application and if applicable, issuing any policy. The answers I have provided are true and accurate;
- 4) I understand that my coverage may be voided by the Insurer if there is any material misrepresentation in my Application, including a misrepresentation as to existing insurance coverage;
- 5) I intend my electronic signature to be the legal equivalent of a handwritten signature and any reproduction of this electronic Application for insurance shall constitute an original when printed from the electronic records of the Insurer;
- 6) I consent to electronic delivery of the policy documents and related information by **(Fillable field for name of MGA)**
- 7) I consent to the collection, use and disclosure of my information by **(Fillable field for name of MGA)** and the insurer, for insurance purposes including but not limited to processing my Application for insurance, arranging for the issuance of the Policy applied for administration and claims. This may mean the insurer will provide some details to third parties, including but not limited to reinsurers, adjusters, service providers and insurance regulatory bodies. I understand that this may also use anonymized elements of data I provided for the analysis of industry trends and to provide benchmarking data.

Please note, The information provided will be treated in confidence and in compliance with all relevant regulation and legislation.

Please review your answers before signing to ensure their accuracy and completeness.

Your completed application will form part of any contract of insurance issued, and cannot be changed.

<b>APPLICANT E-SIGNATURE*</b>	
<b>PRINTED NAME</b>	
<b>JOB TITLE</b>	
<b>EMAIL</b>	
<b>DATE</b>	

\* Must be signed by the authorized signatory: Business Owner, Officer, Director or Manager

---

## Coverage Highlights

---

**Coverage 1: Data Compromise Response Expenses** – covers expenses incurred as the result of the breach of personal information in the custody of the insured or a third-party with whom the insured has a direct relationship. This includes expenses for forensic IT review to determine the nature and extent of the breach, costs to obtain professional legal advice, expenses to notify affected individuals whose information was compromised, cost of services to inform and assist affected individuals in restoring their identity, the cost of professional public relation services to retain the insured's relationship with affected individuals, coverage for the cost of fines or penalties under provincial or federal law, and the cost of payment card industry fines or penalties imposed under contract to which the insured is a party.

**Coverage 2: Identity Recovery** – protects the interests of a key owner of the insured or the spouse of a key owner who become an identity fraud victim. The coverage combines identity theft insurance with services that help victims restore their credit history and identity records to pre-theft status. Coverage reimburses victims for legal expenses, lost wages, child and elder care expenses and miscellaneous fees incurred in resolving problems resulting from identity theft. Includes services such as a toll-free help line and case management assistance to help victims in correcting credit history and identity records.

**Coverage 3a: Computer Attack** – pays for the costs associated with restoring computers and recovering or recreating lost or corrupted data as a result of the insured's discovery of a virus or other computer attack on the insured's devices or network that damages data, software and systems. Includes coverages for restoration of electronic data, recreation of non-electronic data, expenses to restore computer systems to pre-attack functionality, business income loss and extra expenses incurred during the time needed for system and data recovery and restoration, and professional crisis management services for assistance in communicating with outside parties concerning the computer attack and the insured's response.

**Coverage 3b: Loss of Business** – Coverage for business income lost and extra expenses incurred by the insured during the period of time when system and data recovery activities are taking place

**Coverage 4: Cyber Extortion** – provides coverage for the cost of an investigator retained in connection with an extortion threat and coverage for any amount paid by the insured in response to the insured's receipt of a demand for money based on a threat to attack the insured's system, gain access to or release sensitive information (including personally identifying information), or make an unauthorized transfer of funds.

**Coverage 5: Data Compromise Liability** – protects against third-party liabilities the insured might have as a result of a data breach that results in the insured's receipt of a claim, suit or regulatory proceeding, based on a breach of personal information covered under Coverage 1, Data Compromise Response Expenses. Provides coverage for defense costs (within the coverage limit) and settlement costs.

**Coverage 6: Network Security Liability** – pays for costs resulting from the insured's receipt of a claim or suit alleging that a negligent failure of the insured's computer security that allowed one of the following to occur: the breach of business data proprietary to the third party; the unintended propagation of malware to the third party; a denial of service attack against the third party in which the insured unintentionally participated; or the inability of an authorized third party to access the insured's system. Includes coverage for defense costs (within the coverage limit) and settlement costs.

**Coverage 7: Electronic Media Liability** – provides liability coverage as the result of the insured's receipt of a claim or suit alleging that the display of electronic information by the insured on a website resulted in the infringement of another's copyright, title, slogan, trademark, trade name, trade dress, service mark or service name; defamation against a person or organization; a violation of a person's right of privacy; or interference with a person's right of publicity. Liability coverages are provided on a claims-made basis and include defense costs (within the coverage limit) and settlement costs.

**Coverage 8: Misdirected Payment Fraud** – provides coverage for funds lost by the insured as the result of a criminal deception of the insured or the insured's financial institution to induce the insured or the financial institution to send money or divert a payment to a fraudulent destination.

### About HSB

As a member of HSB Group and a proud part of Munich Re, we are a leading provider of Cyber risk insurance, as well as Canada's leading equipment breakdown, and other specialty insurance products and services, to help you grow your business and stay competitive.