

This application form should be completed by Applicants with up to \$25 million in revenue and requiring up to \$1 million policy limits. For higher limit requests or revenues over \$25 million, complete the Custom application form.

By completing this Application Form, the Applicant is applying for insurance with Northbridge Insurance (the "Insurer").

PLEASE READ CAREFULLY: This is an Application for First and Third Party Coverages. If a policy is issued: First Party Coverages are limited to incidents that are first discovered during the policy period; and Third Party Liability Coverages are limited to liability for claims that are first made against the insured during the policy period. The payment of loss, claim expenses (if permitted by law) and first party loss will reduce the Limit of Liability.

All questions must be answered completely. If there is no answer, write "none" or "n/a" in the space provided. Where space provided is insufficient to fully answer, please use separate sheet(s).

A. Information to be completed by all Applicants

Applicant Details

Applicant Name: _____

Address: _____

Business Description: _____

Annual Revenue: _____

URL/Website Address: _____

| | | | | | |
|---|----------|-----------|-----------|-----------|-------------|
| Select Cyber Risk Limit/Aggregate of insurance required: | \$50,000 | \$100,000 | \$250,000 | \$500,000 | \$1,000,000 |
| Select deductible required: | \$1,000 | \$2,500 | \$5,000 | \$10,000 | |

Network Security Best Practices

1. Does the Applicant rely on cloud-based productivity software from Google Workspace or Microsoft 365 on the organization's network(s) with the following features enabled?

| | | |
|---|-----|----|
| 1.1 Filtering all incoming emails and communications for malicious links, spam, malware and attachments? | Yes | No |
| 1.2 Two-factor authentication (2FA) or Multifactor authentication (MFA) enabled on all remote access and emails? | Yes | No |
| 1.3 Google Advanced Protection Program or Microsoft Defender? (combines cloud security, email security and endpoint security) | Yes | No |

If **YES** to all of the above, **skip to Question 4**. If **NO** to any of the above, **proceed to Question 2**.

2. Does the Applicant comply with the following basic security requirements on the organization's network(s)?

| | | |
|---|-----|----|
| 2.1 Running current firewall technology? | Yes | No |
| 2.2 Running anti-virus software? | Yes | No |
| 2.3 Running endpoint security on all connected devices e.g. laptops, mobile devices, desktops? | Yes | No |
| 2.4 Enabling two-factor authentication (2FA) or Multifactor authentication (MFA) enabled on all remote access and emails? | Yes | No |
| 2.5 Filtering all incoming emails and communications for malicious links, spam, malware and attachments? | Yes | No |

Cyber Risk Insurance Application

Backups

3. Does the Applicant have the following protocols in place:

- | | | |
|---|-----------------------------|-----------|
| 3.1 All system configuration and data is subject to regular back-ups via secure cloud? | Yes | No |
| 3.2 All system configuration and data back-ups are maintained in offline copies disconnected from the organization's network? | Yes | No |
| 3.3 All system configuration and data are backed up: | At least weekly | Bi-weekly |
| | Other (describe frequency): | |
| 3.4 Two-factor authentication (2FA) or Multifactor authentication (MFA) settings are enabled for access to file back-ups? | Yes | No |

Software Patches and Updates

4. Does the Applicant have processes in place to implement, within 14 days, all critical security, anti-virus and malware patches received from commercial software vendors deployed to all of its servers, laptops, desktops, routers, firewalls and phones?

Yes No

4.1 Describe frequency if other than within 14 days.

Employee Training

5. Does the Applicant provide all employees with anti-fraud training at least annually (including but not limited to detecting social engineering, phishing, business email compromise and other similar exposures)?

Yes No

Payment Card Compliance

6. Has the Applicant been subject to a PCI investigation? (a check for adherence to standards that businesses follow to secure and protect credit card data conducted by the Payment Card Industry Security Standards Council)

Yes No

6.1 If **YES**, what actions have been taken to ensure compliance?

NO incidents requiring action were identified

Prior Insurance

7. Does the Applicant currently carry Cyber Liability Insurance?

Yes No

If **YES**, complete the following details:

Inception Date: _____

| Insurer | Limit | Deductible | Premium | Retroactive Date |
|---------|-------|------------|---------|------------------|
| _____ | _____ | _____ | _____ | _____ |

Describe any coverage sublimits:

Unknown

None

Cyber Risk Insurance Application

B. Crime (To be completed if optional Cyber Crime is being requested)

| Select sublimit required: | \$10,000 | \$25,000 | \$50,000 | \$100,000 | \$250,000 |
|--|----------|----------|----------|-----------|-----------|
| 8. Does the Applicant conduct, at least annually, awareness training to all employees to recognize and prevent email or phone manipulation techniques that trick users into transferring money or property to fraudsters? | | | | Yes | No |
| 9. Before processing an electronic funds transfer or changing vendor account details, does the Applicant or their employees confirm the request by a secondary means of communication* and using the original contact information on file? | | | | Yes | No |
| <i>*A secondary means of communication is different from the first means of communication. For example, if the request is received by telephone, a secondary communication may be an email.</i> | | | | | |
| 10. Does the Applicant have set dollar limit authorities for employees? | | | | Yes | No |
| 11. Does the Applicant require multiple sign-offs for payments above \$5,000? | | | | Yes | No |

C. Warranty Statements

| | | |
|--|-----|----|
| 12. During the last 5 years, has the Applicant experienced a network security breach, virus or malicious code attack, loss or theft of data (physical or digital), or a hacking or ransomware incident? | Yes | No |
| 13. During the last 5 years, has any loss or any claim been made against the Applicant, whether insured or not, in respect to any of the types of insurance requested in this Application? | Yes | No |
| 14. During the last 5 years, has the Applicant received a complaint regarding content posted online by or on behalf of the Applicant? | Yes | No |
| If YES to any of the questions in section C above, provide full details on a separate sheet, including (i) date of such claim, (ii) claimant's name, (iii) description including incidents and damages alleged, (iv) amount of indemnity and expenses paid and (v) current status & (vi) corrective measures implemented to prevent similar claims. | | |
| 15. Are there any facts, circumstances or situations which could give rise to a claim being made against any insured that may be covered by this Policy? | Yes | No |

Without prejudice to any other rights and remedies of the Insurer, the Applicant understands and agrees that if any such fact, circumstance, or situation exists, whether or not disclosed above in response to Question 15., any claim or action arising from such fact, circumstance or situation will be excluded from coverage under the proposed policy, if issued by the Insurer.

| | | |
|--|-----|----|
| 16. Has the Applicant ever been declined, non-renewed or cancelled by any insurer for Cyber Liability Insurance? | Yes | No |
| If YES , please explain: | | |

D. Declarations

- (i) The Applicant's submission of this Application, and its attachments, does not obligate the Insurer to issue, or the Applicant to purchase a policy. This Application and its attachments shall be the basis of the contract should a policy be issued and shall be deemed to be attached to and form part of the policy. The Insurer is hereby authorized to make any investigation and inquiry in connection with this Application that it deems necessary and is permitted by law.
- (ii) **COVERAGE CANNOT BE BOUND UNLESS THIS APPLICATION FORM HAS BEEN FULLY COMPLETED AND SIGNED.** The undersigned has the power to complete and execute this Application, including Question 15, on behalf of all persons proposed for this insurance and declares that, after inquiry, the statements set forth herein, together with all materials and information submitted or requested by the Insurer, are true.

E. Privacy Disclosure and Consent

The undersigned, on behalf of the insured organization, declares that it has obtained the necessary consent for the collection, use and disclosure by the Insurer of any personal information provided above or in connection with this application or any renewal or change in coverage, for the purposes of offering and providing products and services to meet the insured organization's needs, assessing and underwriting risks on a prudent basis, determining insurance product prices, investigating, and settling claims, detecting and preventing fraud or other illegal activities, analyzing business results and compiling statistics, reporting to regulatory or industry entities, and acting as required or authorized by law.

COMPLETED AND DULY SIGNED AND DATED:

Signed: _____ Please print name: _____
Title: _____ Date: _____