Small Business Cyber Liability Application <$100 Million Annual Revenue

WITH RESPECT TO THE LIABILITY COVERAGES, THE POLICY IS WRITTEN ON CLAIMS MADE AND REPORTED BASIS. COVERAGE UNDER THE POLICY APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY EXTENDED REPORTING PERIOD (IF APPLICABLE) AND REPORTED IN ACCORDANCE WITH THE POLICY CONDITIONS. CLAIM EXPENSES ARE WITHIN AND REDUCE THE LIMITS OF INSURANCE AND ARE SUBJECT TO THE APPLICABLE DEDUCTIBLES.

Instructions

Please respond to questions clearly. Insurers will rely on statements made in this application. This form must be dated and signed within 60 days of the proposed policy inception date.

The term “Applicant” herein refers individually and collectively to all proposed insureds. All responses shall be deemed made on behalf of all proposed insureds.

General Information

Named Insured(s): Primary Website Address:

Applicant’s Street Address:

Names & Websites of all subsidiary companies (if any):

Cybersecurity Contact Name: Email: Phone:

Business Details

1. Insert Applicant’s NAICS Code or description of activities:
2. Most recent fiscal year-end revenue (USD):
3. Current fiscal year-end projected revenue (USD):
4. **[Law Firm Applicants Only]** Number of lawyers:
5. If Applicant purchases professional liability* insurance, please provide the following information from your Policy:

   **Any primary or excess malpractice insurance policy designed to provide the Applicant with coverage for errors or omissions in the delivery or failure to deliver professional services.*

   a. Company Providing Insurance:

   b. Policy Number:

   c. Limit/Deductible:

   d. Retroactive Date:

Computers and Network Security

6. Does the Applicant allow any remote access to connect to its computer network? Yes ☐ No ☐

a. If “Yes”, does the Applicant use multi-factor authentication (“MFA”) for all remote access to the Applicant’s computer network? Yes ☐ No ☐ N/A ☐

b. If "No", and remote access is not allowed, has the Applicant ensured that Remote Desktop Protocol is not accessible via the internet? Yes ☐ No ☐ N/A ☐

7. Does the Applicant download, test, and install security patches within 30 days of release on the Applicant’s computer network (including all hardware and software publicly accessible through the internet)? Yes ☐ No ☐

8. Are all systems and data on the Applicant’s computer network backed up at least weekly? Yes ☐ No ☐

9. Are backups kept fully isolated from the Applicant’s computer systems and network either in: Yes ☐ No ☐
a) offline air-gapped storage; or b) a cloud-based backup service?

Cloud-syncing services such as Dropbox, OneDrive and Google Drive do not qualify as backup services.

10. Does the Applicant operate without any end-of-life or end-of-support hardware or software? Yes ☐ No ☐

If “No”, are those resources segregated from the rest of the computer network? Yes ☐ No ☐ N/A ☐

11. Does the company scan email for potentially malicious attachments and / or links? Yes ☐ No ☐

12. Does the Applicant use any of the following to authenticate incoming email and prevent phishing attacks? Yes ☐ No ☐

- Domain Keys Identified Mail (“DKIM”);
- Sender Policy Framework (“SPF”); or
- Domain-based Message Authentication, Reporting & Conformance (“DMARC”).

13. Does the Applicant encrypt all sensitive or confidential information sent via email or stored on laptops, networked devices, or removable media such as USB drives? Yes ☐ No ☐

14. Are administrative privileges restricted to specific users on the Applicant’s computer network? Yes ☐ No ☐

Shield Up Loss Control Program (Optional)

Applicants are entitled to enroll in the Shield Up cyber loss control program. Shield Up is an easy-to-use online platform that helps Applicants quickly understand cybersecurity requirements and access tools to remediate missing security measures. Additional information is available at www.shieldupcyber.com.

Policyholders enrolled in Shield Up program are entitled to a premium credit when coverage is bound and the Shield Up amendatory endorsement, which broadens coverage. Applicants that enroll in Shield Up must complete the Shield Up onboarding process within 30 days of Policy Inception.

15. Do you wish to participate in the Shield Up program? Yes ☐ No ☐

Cyber Loss History

If the Applicant answers "Yes" to any of the questions below, please complete one Claim Supplement Form (link to form) for each past incident or claim event. For the purposes of the Application questions below, the following terms have special meaning:

- "Security incident" means any breach in security of, unauthorized access to, unauthorized use of, or compromise of, the Applicant's computer systems, including any embezzlement, fraud, theft of private or confidential information, extortion, data or privacy breach, ransomware, denial of service, electronic vandalism or sabotage, computer virus or other similar incidents.
- "System failure" means any interruption, suspension, or impairment of the Applicant's computer system due to:
  A. data creation, entry, or modification errors; or
  B. failures in the on-going operation, administration, upgrading, and maintenance of the Applicant's computer system; or
  C. a voluntary shutdown of the Applicant's computer system to mitigate or avoid potential claims.
- "Multimedia incident" means any:
  A. form of defamation related to disparagement or harm to the reputation, character or feelings of any person or organization;
  B. form of invasion, infringement, or interference with the right to privacy or of publicity;
  C. outrage, outrageous conduct, mental anguish, infliction of emotional distress or prima facie tort; or
  D. infringement of copyright, or the dilution or infringement of trademark, service mark, service name or trade name, actually or allegedly committed by the Applicant or any director, officer, employee or other proposed Insured in the course of online or offline publishing.

16. Has the Applicant had any computer or information security incidents, system failures, or multimedia incidents, during the past three (3) years? Yes ☐ No ☐

17. During the past three (3) years, has the Applicant or any director, officer, employee or other proposed Insured given notice of a claim or circumstances that could give rise to a claim, under the provisions of any prior or current insurance policy, which involve a security incident, system failure, or multimedia incident? Yes ☐ No ☐

18. Does any Applicant, director, officer, employee, or other proposed insured, have knowledge or information of any fact, circumstance, situation, event, or transaction which may give rise to a claim under the proposed insurance? Yes ☐ No ☐

It is understood and agreed that if responses to the "Cyber Loss History" questions are misrepresented or exist and are not disclosed in the Application, any claim, action, or other event or loss based upon, arising out of, or any way involving any such misrepresentation or non-disclosed information is excluded from coverage under the proposed insurance.

Representation Statement

The submission of this Application does not obligate us to issue, or the Applicant to purchase, a Policy. The Applicant will be advised if the Application for coverage is accepted. The Applicant hereby authorizes us to make any investigation and inquiry in connection with this Application that we deem necessary.

The undersigned, acting on behalf of all Applicants, declare that to the best of their knowledge and belief, after reasonable inquiry, the statements set forth in this Application and any attachments or other documents submitted with the Application are true and complete and no material facts have been withheld. A material fact is one in which the knowledge or ignorance of it would naturally and reasonably influence the judgment of an insurer in making the contract at all, in estimating the degree or character of the risk, in fixing the rate of premium, or would otherwise be deemed material under applicable law.

The undersigned agree that the information provided in this Application and any material submitted herewith are the representations of all the Applicants and the basis for issuance of the insurance Policy should a Policy providing the requested coverage be issued, and that we will have relied on all such materials in issuing any such Policy. The undersigned further agrees that the Application and any material submitted herewith shall be considered attached to and a part of the Policy.

The undersigned hereby acknowledge they are aware that:

1. The information requested in this Application is for underwriting purposes only and does not constitute notice to us of a claim, or a potential claim, under any Policy underwritten by us; and
2. As part of our underwriting and/or loss control processes, we may scan or otherwise assess the internet-exposed resources on the Applicant's computer network for vulnerabilities using risk assessment tools; and
3. The Limits of Insurance in the Policy for which this Application is made will be reduced and may be completely exhausted, by amounts incurred for legal defense costs. We shall not be liable for the legal defense costs, the amount of any judgment or settlement, or any other costs and expenses, to the extent that such costs exceed the Limits of Insurance of this Policy; and
4. All legal defense costs, the amount of any judgment or settlement, or any other costs and expenses, which are incurred under the Policy for which this Application is made, are subject to the applicable Deductible under the Policy.

The undersigned further agrees that if the information supplied on this Application changes between the date this Application is signed and the date of Policy issuance, the Applicant shall immediately notify us of such changes. We may then withdraw or modify outstanding quotations and/or authorization or agreement to bind this insurance.

Name: ***Title:***

Email:

Signed: ***Date:***

Notice to New York Applicants: Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime and shall also be subject to: a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

Notice for all other Applicants: Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance may be guilty of a crime.

Operational Technology Application Supplement Form

Instructions

Please respond to answers clearly. Insurers will rely on statements made in this Supplement. This form must be signed and dated.

The term “Applicant," herein refers individually and collectively to all proposed insureds; all responses shall be deemed made on behalf of all proposed insureds.

Applicants in the classes of business listed below must complete the OT application supplement.

- Energy (Oil, Gas & Consumable Fuels)
- Engineering
- Food and Beverage Production
- Manufacturing
- Wholesale Trade

1. Select the type(s) of operational technology (OT) assets that exist within the Applicant’s organization: (select all that apply)

- ☐ Industrial Control Systems (ICS) or Supervisory Control & Data Acquisition (SCADA)
- ☐ Critical Internet of Thing Devices (IoT) devices (door locks/actuators, smoke detectors, etc.)
- ☐ Non-Critical Internet of Thing (IoT) devices
- ☐ Terminals (ATMs, kiosks, payment terminals, etc.)
- ☐ None of the above

2. For any assets selected in question 1, are those systems and/or devices segregated from the rest of the Applicant’s IT network? Yes ☐ No ☐

If IT and OT assets are partially segregated, please provide details on page 5.

3. Can the applicant’s operational technology (OT) assets be controlled remotely via the internet, VPN, Bluetooth and/or a third-party connection? Yes ☐ No ☐

If yes, do you require multi-factor authentication (MFA) to access these assets remotely? Yes ☐ No ☐ N/A ☐

Representation Statement

By signing this document, the undersigned authorized representative of the Applicant represents on behalf of all persons and entities proposed for coverage, after inquiry, that to the best of their knowledge, the statements and answers given in and all materials submitted with this Application are true, accurate and complete.

Signed: ***Date:***

Additional Information

Use this space to provide any details to your responses.