CYBER INSURANCE APPLICATION

IMPORTANT NOTICE

By completing this Application, the Applicant is applying for a Cyber Insurance Policy which provides coverage for claims first made against any Insured during the Policy Period, or any applicable Extended Reporting Period, and reported to the Insurer pursuant to the terms of this Policy.

Please read the entire Application and Policy carefully before signing.

Whenever used in this Application, the term "Applicant" shall mean the Named Insured and all Subsidiaries, unless otherwise stated. All terms which appear in bold type herein are used in this Application with the same respective meanings as set forth in the Cyber Insurance Policy.

The information provided in this application will be used to evaluate the cyber risk profile and determine appropriate coverage and pricing.

A. Applicant Information

1. Legal name of Applicant:

_____

2. Primary industry / description of operations:

_____

3. Headquarters address:

_____

4. Primary website domain(s):

_____

5. Total employees:

_____

6. Annual revenue (most recent FY):

_____

B. Data & Systems

1. How many unique records containing personal data do you store or process?

_____

2. Do you store or process biometric data?..... ☐ Yes ☐ No

3. Do you accept or process payment cards?..... ☐ Yes ☐ No

If Yes, are you or your processor PCI compliant?..... ☐ Yes ☐ No

4. Are your critical systems primarily:

☐ Cloud-based
☐ On-premises
☐ Hybrid

5. Do you have a process to classify or secure sensitive data?..... ☐ Yes ☐ No ☐ NA

6. Do you have written contracts with third-party data processors?..... ☐ Yes ☐ No ☐ NA

7. Do vendors handling sensitive data undergo security review?..... ☐ Yes ☐ No ☐ NA

C. Access Security

1. Is Multi-Factor Authentication (MFA) required for:

Email access: ..... ☐ Yes ☐ Partial ☐ No
Remote access (VPN/RDP/etc.): ..... ☐ Yes ☐ Partial ☐ No
Admin / privileged accounts: ..... ☐ Yes ☐ Partial ☐ No

2. Do end users have local administrator rights?..... ☐ Yes ☐ No

3. Is Single Sign-On (SSO) in place?..... ☐ Yes ☐ No

4. Do you use a Privileged Access Management (PAM) tool?..... ☐ Yes ☐ No

5. Do you use a password manager for staff?..... ☐ Yes ☐ No

D. Endpoint & Network Security

1. What endpoint protection do you use? (e.g., Microsoft Defender, CrowdStrike, SentinelOne, Sophos, Carbon Black)

_____

2. Is Endpoint Detection & Response (EDR) deployed on all workstations/servers?

☐ Yes
☐ No
☐ Partial _____ % of network covered

3. Do you have Managed Detection & Response (MDR) or 24/7 SOC monitoring?..... ☐ Yes ☐ No

4. Is your network segmented to limit lateral movement?..... ☐ Yes ☐ No

5. Do you use email security measures (e.g., filtering, spoofing protection such as SPF/DKIM/DMARC)?

☐ Yes
☐ Partial
☐ No

E. Patch & Vulnerability Management

1. Do you track and apply critical security patches?..... ☐ Yes ☐ No

2. Critical patches deployed within:

☐ <1 week
☐ <30 days
☐ >30 days or NA

3. Do you conduct vulnerability scans?..... ☐ Yes ☐ No

4. Do you have any end-of-life operating systems or software in use?..... ☐ Yes ☐ No

If Yes, how are they isolated or protected? _____

F. Backup, Continuity & Incident Response

Backups

1. Do you maintain regular data backups?..... ☐ Yes ☐ No

2. Backup frequency:

- ☐ Continuous
- ☐ Daily
- ☐ Weekly

3. Are backups tested regularly?..... ☐ Yes ☐ No

4. Where are backups stored?

- ☐ On-premises
- ☐ Cloud
- ☐ Offsite
- ☐ Offline

5. How are backups protected?

- ☐ Encrypted Backups
- ☐ MFA Potected Backups
- ☐ Immutable Backups

6. Have you completed a full restore test in the last 12 months?

☐ Yes ☐ No

Business Continuity & IR

1. Do you maintain a formal Incident Response Plan?..... ☐ Yes ☐ No

If yes, has it been tested in the last 12 months?..... ☐ Yes ☐ No

2. Do you have a Business Continuity or Disaster Recovery Plan?..... ☐ Yes ☐ No

If yes, has it been tested in the last 12 months?..... ☐ Yes ☐ No

E. Training & Email Security

1. Do employees receive annual cybersecurity training?..... ☐ Yes ☐ No

2. Do you run phishing tests?..... ☐ Yes ☐ No

3. Do you have an easy way for employees to report suspicious email? ..... ☐ Yes ☐ No

4. Are external emails flagged?..... ☐ Yes ☐ No

G. History & Claims

1. Any cyber incidents, privacy breaches, fund-transfer fraud, or system outages in last 3 years?..... ☐ Yes ☐ No

2. Are you aware of any current circumstances that could lead to a claim?..... ☐ Yes ☐ No

If Yes to question 1. Or 2. , provide brief details:

_____

H. Signature

I confirm the statements in this application are accurate and complete.

Name: _____

Title: _____

Date: _____

Signature: _____

FRAUD WARNING

NOTICE TO ALL 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, for the purpose of misleading, conceals information concerning any fact material thereto, may commit a fraudulent insurance act which is a crime and may subject such person to criminal and civil penalties.