APPLIED
FINANCIAL LINES

AFL-CYB-APP-2025
Applied Financial Lines
appliedfinanciallines.com

Cyber Insurance Application

Comprehensive Risk Assessment

IMPORTANT NOTICE: This policy provides coverage on a **claims-made and reported basis** and applies only to claims first made against the Insured during the Policy Period or Extended Reporting Period, if purchased, and reported to the Insurer in accordance with the terms of the Policy. Defense costs are included within the Limit of Liability and will reduce and may exhaust the Limit of Liability.

Please read the entire Application and Policy carefully before signing. If a policy is issued, this Application will attach to and become part of the Policy.

1 Applicant Information

LEGAL NAME OF APPLICANT

PRIMARY INDUSTRY / DESCRIPTION OF OPERATIONS

HEADQUARTERS ADDRESS

PRIMARY WEBSITE / EMAIL DOMAIN(S)

TOTAL NUMBER OF EMPLOYEES

ANNUAL REVENUE (MOST RECENT FISCAL YEAR)

$

REQUESTED POLICY EFFECTIVE DATE

1.1 Do you have subsidiaries you want covered under this policy? ☐ Yes ☐ No

> *If Yes, please attach a list of subsidiaries with addresses and revenues.*

2 Data & Systems

A. Sensitive Data

2.1 Estimated number of records containing PII, PHI, or financial data stored or processed: (choose one)

◯ <250,000 ◯ 250K – 1M ◯ 1M – 5M ◯ >5M

2.2 Do you store or process biometric data? ☐ Yes ☐ No

2.3 Do you accept or process payment cards? ☐ Yes ☐ No

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

B. Data Controls

2.4 Do you have a process to classify and secure sensitive data? ☐ Yes ☐ No ☐ N/A

2.5 Do you have written contracts with third-party data processors? ☐ Yes ☐ No ☐ N/A

2.6 Do vendors handling sensitive data undergo security review? ☐ Yes ☐ No ☐ N/A

C. Infrastructure

2.7 Primary critical system environment: (choose one)

◯ Cloud-based ◯ On-premises ◯ Hybrid

3 Access Security

A. Multi-Factor Authentication (MFA)

3.1 Is Multi-Factor Authentication required for the following?

Email access (Office 365, Gmail, etc.)	☐ Yes	☐ Partial	☐ No
Remote access (VPN, RDP, Citrix, etc.)	☐ Yes	☐ Partial	☐ No
Admin / Privileged accounts	☐ Yes	☐ Partial	☐ No

B. General Access Controls

3.2 Do end users have local administrator rights on their workstations? ☐ Yes ☐ No

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

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

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

4 Endpoint & Network Security

A. Endpoint Protection

4.1 What endpoint protection solution do you use?

(e.g., CrowdStrike, Microsoft Defender, SentinelOne, Sophos, Carbon Black)

4.2 Is Endpoint Detection & Response (EDR) deployed on all workstations and servers? ☐ Yes ☐ No

If Yes, what percentage of endpoints are covered? _____ %

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

B. Network Security

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

4.5 Do you use email security measures (filtering, SPF/DKIM/DMARC)? ☐ Yes ☐ No

4.6 Do you use remote access tools (VPN, RDP)? ☐ Yes ☐ No

If Yes, please specify:

5 Patch & Vulnerability Management

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

5.2 Critical patches are typically deployed within: (choose one)

◯ <1 Week ◯ 1–4 Weeks ◯ >30 Days

5.3 Do you conduct vulnerability scans? ☐ Yes ☐ No

If Yes, how frequently?

◯ Monthly ◯ Quarterly ◯ Annually

5.4 Do you have any end-of-life operating systems or software in production? ☐ Yes ☐ No

If Yes, how are they isolated or protected?

6 Backup, Continuity & Incident Response

A. Backup Strategy

6.1 Do you maintain regular data backups? ☐ Yes ☐ No

6.2 Backup frequency: (choose one)

- ◯ Continuous ◯ Daily ◯ Weekly ◯ Monthly

6.3 Where are backups stored? (select all that apply)

- ☐ On-premises
- ☐ Cloud
- ☐ Offsite
- ☐ Offline / Air-gapped

6.4 How are backups protected? (select all that apply)

- ☐ Encrypted
- ☐ MFA-protected access
- ☐ Immutable backups

6.5 Are backups tested regularly? ☐ Yes ☐ No

6.6 Have you completed a full restore test in the last 12 months? ☐ Yes ☐ No

B. Incident Response & Business Continuity

6.7 Do you have a formal Incident Response Plan? ☐ Yes ☐ No

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

6.8 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

7 Training & Awareness

7.1 Do employees receive annual cybersecurity awareness training? ☐ Yes ☐ No

7.2 Do you conduct phishing simulation tests? ☐ Yes ☐ No

7.3 Do employees have an easy way to report suspicious emails? ☐ Yes ☐ No

7.4 Are external emails flagged or tagged? ☐ Yes ☐ No

8 Third-Party & IT Management

8.1 Do you outsource IT or security management (MSP/MSSP)? ☐ Yes ☐ No

If Yes, please provide provider name:

8.2 Do you use cloud-hosted applications (Microsoft 365, Google Workspace, AWS, etc.)? ☐ Yes ☐ No

9 Loss History & Prior Claims

9.1 In the past 3 years, has the Applicant experienced any cyber incident, privacy breach, funds transfer fraud, or significant system outage? ☐ Yes ☐ No

9.2 Are you aware of any current circumstances that could reasonably give rise to a claim under this policy? ☐ Yes ☐ No

If Yes to either question above, please provide details:

Note: If the Applicant has knowledge of any fact, circumstance, or situation that may give rise to a claim under this policy, any claim arising therefrom is excluded from coverage.

10 Representations & Signature

The undersigned authorized representative of the Applicant declares that: (1) this Application has been completed after reasonable inquiry; (2) the statements set forth herein are true and complete to the best of their knowledge; and (3) these declarations are a material inducement to the Insurer to provide a proposal for insurance.

The undersigned agrees that if the information supplied on this Application changes between the date of this Application and the effective date of the insurance, the Applicant will immediately notify the Insurer of such changes, and the Insurer may withdraw or modify any outstanding quotations or authorizations.

NAME OF AUTHORIZED REPRESENTATIVE

TITLE

SIGNATURE

DATE (MM/DD/YYYY)

EMAIL ADDRESS

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.

AFL-CYB-APP-2025