CYBER INSURANCE APPLICATION
Comprehensive Risk Assessment

1. APPLICANT INFORMATION

Legal Name: _____   **Total Employees:** _____

Industry: _____   **Annual Revenue:** $_____

Address: _____   **Website(s):** _____

	Yes	No
Do you own subsidiaries you want covered?	☐	☐

(If Yes, attach list)

2. DATA & SYSTEMS

A. Record Counts (Estimate number of records containing PII, PHI, or Financial Data)

	<250k	250k-1M	1M-5M	>5M
How many sensitive records do you store?	☐	☐	☐	☐

B. Data Controls

	Yes	No
Do you store or process biometric data?	☐	☐
Do you accept or process payment cards (PCI)?	☐	☐
If Yes, are you PCI compliant?	☐	☐
Do you classify and secure sensitive data?	☐	☐

C. Infrastructure

	Cloud	On-Prem	Hybrid
Primary critical system environment:	☐	☐	☐

3. ACCESS SECURITY

Is Multi-Factor Authentication (MFA) required for:

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

General Access Controls:

	Yes	No
Do end users have local administrator rights?	☐	☐
Is Single Sign-On (SSO) in place?	☐	☐
Do you use a Privileged Access Management (PAM) tool?	☐	☐
Do you use a password manager for staff?	☐	☐

4. ENDPOINT & NETWORK SECURITY

Endpoint Protection Tool Used: _____

(e.g., CrowdStrike, Defender, SentinelOne)

	Yes	Partial	No
Is EDR deployed on all endpoints?	☐	☐	☐
Do you use email security (SPF/DKIM/Filtering)?	☐	☐	☐

	Yes	No
Do you have Managed Detection & Response (MDR) / 24/7 SOC?	☐	☐
Is your network segmented to limit lateral movement?	☐	☐
Do you use remote access tools (VPN, RDP)?	☐	☐

(If Yes, list below)

_____

5. PATCH & VULNERABILITY MANAGEMENT

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

Deployment Timing (Critical Patches):

	<**1 Week**	<**30 Days**	>**30 Days**
Time to deploy critical patches:	☐	☐	☐

Vulnerability Scanning:

	Monthly	**Quarterly**	**Annually**
Scan Frequency:	☐	☐	☐

6. BACKUP, CONTINUITY & INCIDENT RESPONSE

Backup Strategy

	Yes	No
Do you maintain regular data backups?	☐	☐

Frequency: .... **Continu-ous** ☐   **Daily** ☐   **Weekly** ☐

	Yes	No
Are backups tested regularly?	☐	☐
Do you maintain **offline / air-gapped / immutable** backups?	☐	☐
Are backups encrypted?	☐	☐
Have you completed a full restore test in the last 12 months?	☐	☐

Planning

	Yes	No
Do you have a formal Incident Response Plan?	☐	☐
Tested in last 12 months?	☐	☐
Do you have a Business Continuity / Disaster Recovery Plan?	☐	☐

7. THIRD-PARTY & PERSONNEL

	Yes	No
Do you outsource IT/Security (MSP/MSSP)?	☐	☐
Do you use cloud-hosted apps (M365, AWS, etc.)?	☐	☐
Do employees receive annual cyber training?	☐	☐
Do you run phishing tests?	☐	☐
Are external emails flagged?	☐	☐

8. HISTORY & CLAIMS

	Yes	No
Any cyber incidents, breaches, or claims in the last 3 years?	☐	☐
Are you aware of any circumstances that could lead to a claim?	☐	☐

If Yes, please provide details:

_____

3

9. SIGNATURE

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

Name: _____   **Title:** _____   **Date:** _____

Signature: _____