CYBER INSURANCE READINESS CHECKLIST

IT Security Requirements for Cyber Insurance Coverage

This checklist summarizes the key IT security measures evaluated by insurance underwriters when assessing an organization's eligibility for cyber and privacy security coverage. Meeting these requirements positions your business for the strongest coverage and most favorable premiums.

POLICIES & PLANS

- ☐ Written Information Security Program (WISP) *Formal, documented policy governing how you protect data and systems*
- ☐ Written Incident Response Plan *Documented plan for responding to a cyber breach or attack*
- ☐ Disaster Recovery Plan *Fully documented and tested at least annually; covers hardware, software, network, and data*
- ☐ Identified Security Individual *Or equivalent role responsible for information security oversight*
- ☐ Written Data Retention & Destruction Policy *Responsible disposal of computers, devices, and media when no longer needed*

TRAINING & AWARENESS

- ☐ Formal & Documented Security Training *Written and executed employee training program to safeguard personal and confidential information*
- ☐ Social Engineering Training *Annual training for employees with wire transfer/AP authority on detecting fraudulent emails and phone calls*

TECHNICAL CONTROLS

- ☐ Firewalls *Both hardware AND software firewalls deployed*
- ☐ End Point Detections and Response (EDR) *Real time monitoring and response to advanced cyber threats, helping detect and stop attacks before they spread.*
- ☐ Encryption *Deployed for data at rest, in transit, AND on mobile devices*
- ☐ Patching & Updates *Automatic updates enabled with patch management verification procedures*
- ☐ Email Security *Both web AND email filtering enabled*
- ☐ Multi-Factor Authentication (MFA) *Required when employees/contractors access critical systems*
- ☐ VPN with MFA for Remote Access *Remote employees access a segmented network via VPN with multi-factor authentication*
- ☐ Backups *Regular full AND incremental backups of critical data and systems*

ACCESS & ACCOUNTABILITY

- ☐ Unique Accounts with Strong Passwords & Least Privilege *Separate accounts for all users; access restricted and extended only as required for duties*
- ☐ Background Checks *Full nationwide criminal, sex offender, and credit checks for employees with access to sensitive data/systems*

PHYSICAL & FACILITY SECURITY

- ☐ Key Card Access & Protocols *Controlled building and room access via key card systems*
- ☐ 24-Hour Security Surveillance *Continuous monitoring of facilities*
- ☐ Biometric Scanning *Biometric authentication for secure areas*
- ☐ Redundant Infrastructure *Redundant network equipment, connectivity, power, and cooling*
- ☐ Security Personnel *Facilities security manager and/or security guards*

VENDOR & THIRD-PARTY MANAGEMENT

- ☐ Vendor Security Requirements in Contracts *Security responsibilities for sensitive/confidential info addressed in all vendor and partner agreements*
- ☐ Formal Vendor Review Process *Documented procedures for reviewing vendors' security practices*
- ☐ Written Procedures for Vendor Payment Changes *Employees must authenticate all vendor bank/routing changes via phone call to an authorized rep*
- ☐ Vendor E&O Insurance Requirements *Vendors required to carry errors and omissions insurance*

DATA GOVERNANCE

- ☐ Data Classification & Inventory *Identify and classify all sensitive records: biometric, financial, PII/SSN, PHI, credit cards*
- ☐ Website Privacy Controls *Users have opt-in/opt-out options for collection and use of their information*
- ☐ PCI-DSS Compliance *Outsource payment processing to a PCI-DSS validated merchant or maintain PCI certification*

Source: Hanover Insurance Group — Technology Professional and Cyber Advantage Underwriting Application (Form 114-10154)