Cyber Readiness Checklist

Prepared by SignalHaven Compliance

Date: May 18, 2025

Use this checklist to quickly assess whether your business has the basic cybersecurity controls and documentation required for cyber insurance eligibility and best practices compliance.

1. Cybersecurity Policies

[ ] Acceptable Use Policy is documented and enforced

[ ] Password Policy is in place and communicated

[ ] Incident Response Plan is documented and accessible

[ ] Data Protection and Handling Policy is available to staff

2. Technical Safeguards

[ ] Multi-Factor Authentication (MFA) is enabled for email and critical systems

[ ] Antivirus or endpoint protection is installed on all devices

[ ] Data backups are performed regularly and tested

[ ] Firewalls or network protection are configured and monitored

3. Employee Readiness

[ ] Employees have received basic cybersecurity training

[ ] Employees know how to identify phishing emails

[ ] There is a known process for reporting suspicious activity

4. Compliance & Risk

[ ] Business has reviewed insurance cybersecurity requirements

[ ] Third-party vendors are evaluated for security practices

[ ] Systems and software are kept up to date with patches

This checklist is a starting point. For a full cybersecurity readiness assessment or assistance preparing policies, contact SignalHaven Compliance at contact@signalhavencompliance.com or visit signalhavencompliance.com.