



INSURABILITY CHECKLIST

Your Business, Your Mission, Secured!

Identifying and Addressing Risk & Resiliency for your technologies, to meet your business objectives.

Cybersecurity Insurability Checklist: Foundational Questions for Underwriting Requirements

If you are an organization seeking Cyber Liability Insurance, you should be able to answer “Yes” to all of the following questions. Please contact Fidus if you have questions or are in need of assistance at: Services@FidusCyber.com

Access Controls:

- Have you established separate accounts for administrator and user credentials?
- Are local administrator permissions removed for all users except authorized system administrators?
- Do you require all users to use Multi-Factor Authentication (MFA) to authenticate when accessing critical systems, applications or company data?
- Is MFA leveraged consistently across the organization (e.g., networks, email, applications, remote access)? If not, where & why not?

Encryption:

- Do you encrypt sensitive data at rest?
- Do you encrypt sensitive data in motion?
- Do you require emails to be encrypted?
- Do you require disc encryption on all endpoints?

Identity Access Management:

- Do you perform a regular review & audit of staff and administrator access credentials?
- Are user accounts and permissions actively managed and regularly audited?
- Does your access management process leverage the principle of least privileged?
- Do you require separate accounts for user and administrator?

Monitoring:

- Do you have visibility and governance of organization’s Software as a Service (SaaS), (e.g., CRM, HRIS, ERP, etc.)?
- Do you use an Endpoint Detection & Response (EDR) tool?
- Is the tool managed/monitored internally or by a 3rd party vendor?
- Is an alerting process implemented? Who performs the reviews to actively detect threats?

Resiliency:

- Do you have a documented & tested formal Incident Response Plan?
- Do you have a Business Continuity Plan?
- Do you have a Disaster Recovery Plan?

Security Awareness:

- Do you have an established Security Awareness Training program? If yes, is it provided internally or by a 3rd party vendor?
- What is the training frequency? Is training completion tracked?
- Do you perform Phishing testing? Are results tracked and remedial training issued where required?

System & Data Backups:

- Do you have an established backup process? How often do you perform your backups?
- Are the backups stored offsite? Are they isolated?
- Are your backups encrypted?
- Are your backups immutable?
- How often do you test your backups?

Vulnerability Management & Patching:

- Do you actively scan for vulnerabilities by performing restoration testing?
- Are vulnerabilities tracked? Do you follow a prioritization of vulnerability remediation?
- Do you have a central patch management process to ensure critical updates are applied?

Penetration Testing:

- Have you leveraged internal or external Penetration Testing?
- Do you perform Penetration Testing once or twice a year?