CYBER READINESS CHECKLIST

A quick self-assessment to evaluate your cybersecurity posture

1. Access & Authorization

Multi-Factor Authentication (MFA) is enforced for:

- □ Email
- □ VPN
- □ Cloud services (e.g., Microsoft 365)
- □ Remote access and admin accounts

2. Data Backup

- □ Backups are performed regularly (daily or weekly)
- □ Backups are stored offsite or in the cloud
- □ Backups are encrypted
- □ Backup restoration processes are tested quarterly

3. Endpoint Protection

- □ All endpoints (laptops, desktops, servers) have up-to-date antivirus/anti-malware
- □ Endpoint Detection & Response (EDR) or Next-Gen AV is in place
- □ Devices are regularly patched and updated

4. Monitoring & Incident Response

- □ A system is in place to monitor for threats or unusual behavior
- □ An Incident Response Plan (IRP) is documented and accessible
- □ Employees know who to report cyber incidents to

5. Security Awareness Training

- □ Employees receive cybersecurity training at least annually
- □ Simulated phishing tests are conducted to raise awareness
- □ Training includes password hygiene, phishing, and data handling

6. Privileged Access & Password Management

- □ Admin access is restricted and monitored
- □ Passwords are managed securely (e.g., via a password manager)
- □ Default passwords are changed immediately after setup

7. Policies & Compliance

- □ Acceptable Use and Security Policies are documented and distributed
- □ Regular reviews ensure compliance with frameworks like NIST, CIS Controls, or ISO 27001
- □ Cyber liability insurance requirements are reviewed annually

Calculate Your Score

Give yourself 1 point for every box checked.

20–23 points - Strong cybersecurity posture
12–19 points - Moderate risk - gaps to address
0–11 points - High risk; significant vulnerabilities

We are **provenIT**

provenIT.com ☎ 708.614.1770