CAPTAIN I.T.

CYBERSECURITY CHECKLIST

Cybersecurity is critical to protecting your business from data breaches, ransomware, and other digital threats. This checklist will help ensure your organization is taking the necessary steps to safeguard sensitive information, secure networks, and comply with regulatory requirements. Use it as a foundation for your internal audits or when evaluating your cybersecurity readiness.

Network Security

- □ Firewall configured and regularly reviewed
- □ Intrusion Detection/Prevention System (IDS/IPS) deployed
- □ Secure remote access via VPN or Zero Trust Network Access
- □ Wi-Fi networks segmented and secured with strong encryption
- □ Network devices (routers, switches) updated and password-protected

Endpoint Protection

- □ Antivirus and antimalware software installed and up-to-date
- □ Real-time threat detection and response in place
- □ Automatic updates enabled for all operating systems and applications
- □ Device encryption enabled (BitLocker, FileVault, etc.)
- □ Lost/stolen device policy and tracking in place

Access Controls

- □ Multi-factor authentication (MFA) enabled for all users
- □ Role-based access controls (RBAC) implemented
- □ Inactive accounts removed or disabled
- □ Strong password policies enforced
- □ User access reviewed quarterly

Data Protection

- □ Sensitive data encrypted in transit and at rest
- □ Data classification policies established
- □ Backups performed daily and stored securely offsite
- □ Data loss prevention (DLP) tools implemented
- □ Tested and documented disaster recovery procedures

Security Monitoring & Response

- □ Security Information and Event Management (SIEM) system in place
- □ Centralized log collection and review process established
- □ Incident response plan developed and tested
- □ Employees trained on how to report suspicious activity
- □ External threat intelligence integrated into monitoring tools

User Awareness & Training

- □ Ongoing cybersecurity training for all employees
- □ Phishing simulations conducted regularly
- □ Acceptable use policy distributed and acknowledged
- □ Social engineering awareness training completed
- □ Security best practices included in onboarding process

Compliance & Audits

- □ Regular security audits and vulnerability scans conducted
- □ Policies aligned with compliance frameworks (HIPAA, CMMC, PCI-DSS, etc.)
- □ Third-party vendor risk assessments completed
- □ Cyber insurance policy reviewed annually
- □ Compliance documentation updated and accessible

Need Help Securing Your Business?

Don’t leave your cybersecurity to chance. Partner with Captain IT for a comprehensive, proactive approach to protecting your data, systems, and reputation.

Contact us for a free consultation!

✉ Hello@CaptainIT.com ☎ (800) 834-9795