CAPTAIN I.T.

NETWORK SECURITY CHECKLIST

Securing your network is one of the most critical aspects of protecting your business from cyber threats. This checklist aligns with the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) and provides a detailed guide to ensure your network infrastructure is secure, compliant, and resilient. By following these best practices, you can strengthen your cybersecurity posture and reduce risk across your environment.

Perimeter Security

- □ Firewall configured and actively monitored
- □ Intrusion Detection and Prevention Systems (IDS/IPS) deployed
- □ Router and switch configurations secured (no default credentials)
- □ Port forwarding and open ports reviewed regularly

Access Controls

- □ Role-based access controls (RBAC) implemented
- □ Multi-factor authentication (MFA) enforced for critical systems
- □ VPN access secured and restricted to authorized users
- □ Network segmentation in place to isolate sensitive systems

Endpoint Security

- □ All endpoints have up-to-date antivirus and anti-malware software
- □ Endpoint Detection and Response (EDR) tools deployed
- □ Remote wipe capabilities for lost/stolen devices
- □ Patch management processes for all endpoints

Monitoring & Logging

- □ Centralized logging of all network activity
- □ Log retention policies meet compliance standards
- □ Alerts configured for unusual network behavior
- □ SIEM (Security Information and Event Management) tool in use

Wireless Security

- □ Wireless networks use WPA3 or WPA2 encryption
- □ Guest Wi-Fi isolated from internal network
- □ Wireless access point firmware regularly updated
- □ SSID broadcasting policies reviewed and enforced

Email & Web Security

- □ Spam filtering and phishing protection in place
- □ Web filtering to block malicious or non-business sites
- □ Email attachment scanning for malware
- □ DMARC, DKIM, and SPF records configured properly

Policies & Training

- □ Network security policy documented and distributed
- □ Employee cybersecurity awareness training provided
- □ Acceptable use policies signed and reviewed annually
- □ Incident response plan includes network breach scenarios

Need Help Strengthening Your Network Security?

Your network is the foundation of your IT infrastructure—don’t leave it vulnerable. Captain IT provides expert network security assessments and proactive protection to keep your business safe.

Contact us for a FREE consultation!

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