CAPTAIN I.T.

# ENDPOINT SECURITY AUDIT CHECKLIST

Endpoints such as laptops, desktops, and mobile devices are often the first target for cyber threats. Conducting a regular Endpoint Security Audit is essential to identify vulnerabilities, ensure proper configurations, and protect your business from ransomware, data breaches, and insider threats. Use this checklist to assess the security posture of your organization's endpoints and enforce best practices.

## Antivirus & Anti-Malware

- □ Verified installation of up-to-date antivirus/anti-malware software
- □ Scheduled scans are configured and running
- □ Real-time protection is enabled
- □ Antivirus definitions are updated regularly
- □ Tamper protection is enabled for endpoint security software

## Patch & Update Management

- □ Operating systems are fully patched and up to date
- □ Third-party applications are updated regularly
- □ Automatic updates are enabled where applicable
- □ Audit trail of update history maintained

## Access Control & Authentication

- □ Unique user accounts for all endpoint users
- □ Multi-factor authentication (MFA) enforced
- □ Account lockout policies configured
- □ Administrator privileges are limited
- □ Idle session timeouts and auto-lock enabled

## Endpoint Encryption

- □ Full disk encryption (e.g., BitLocker, FileVault) enabled
- □ Removable media encryption enforced
- □ Encryption key management policies in place
- □ Email and file transmission encryption policies enforced

## Network & Remote Access

- □ Firewalls enabled and configured on all endpoints
- □ Secure VPN required for remote access
- □ Public Wi-Fi usage policies enforced
- □ Network traffic monitoring and filtering tools deployed

## Mobile Device Security

- □ Mobile Device Management (MDM) system in place
- □ Remote wipe capabilities enabled
- □ Application control and restrictions implemented
- □ Lost/stolen device reporting policy enforced

### Monitoring & Logging

- □ Endpoint activity logging enabled
- □ Alerts configured for suspicious behavior
- □ SIEM or centralized logging tool in use
- □ Audit logs reviewed regularly

### User Awareness & Policy Compliance

- □ Users trained on endpoint security best practices
- □ Acceptable Use Policies (AUP) signed by all users
- □ Regular phishing simulations conducted
- □ Incident response procedures communicated and tested

## Protect Every Endpoint – Stay Secure!

Your business is only as secure as its weakest endpoint. Let Captain IT help you harden your systems and stay ahead of evolving cyber threats with a professional endpoint security audit.

### Contact us for a FREE consultation!

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