Essential Cybersecurity Checklist for Businesses

mother technologies

Your Business Protection Checklist

In today's digital landscape, businesses of every size face the threat of cyberattacks. Cybercriminals target not only small companies with weak defences but also larger organisations with valuable data. To avoid costly downtime, financial losses, and damage to your reputation, it's crucial to implement effective security measures.

This checklist highlights essential cybersecurity steps that every business should take to enhance its protection. By following these guidelines, you can safeguard your operations and strengthen your defences against potential threats.

Secure your Accounts

01 **Enable Two-Factor Authentication (2FA):** Wherever possible, ensure that 2FA is turned on for all critical business accounts, especially those related to finance, email, and data. We recommend using Cisco Duo as your 2FA authenticator app for enhanced security. ☐

02 **Use Strong, Unique Passwords:** Implement a password manager to generate and securely store strong passwords for each account, reducing the risk of password reuse across systems. ☐

03 **Minimise Shared Accounts:** Reduce the use of shared accounts, and ensure that any shared accounts are properly secured. Assign individual credentials to users to enhance accountability. ☐

04 **Enforce Access Control:** Ensure that users only have access to the systems and data necessary for their roles. Review access rights regularly to prevent unnecessary access. ☐

Protect your Devices and Information

05 **Automatic Software Updates:** Set up all devices, including servers and endpoints, to automatically install updates and patches. This helps protect against vulnerabilities in outdated software. ☐

06 **Data Backups:** Reliable backups are essential for protecting your business from attacks. Businesses should establish a regular backup routine, storing backups both onsite and in the cloud. ☐

07 **Endpoint Detect & Response:** Standard antivirus software isn't enough to protect against advanced threats. Use RoundClock EDR, powered by industry leader **SentinelOne**, which leverages AI to monitor devices in real-time, detecting and responding to threats as they emerge. ☐

08 **Next Generation Firewall for your Network:** NGFWs go beyond traditional firewalls by offering deep traffic analysis to defend against evolving cyberattacks. Our RoundClock NGFW is powered by **Cisco Meraki.** ☐

09 **DNS Filtering on All Devices & Networks:** Implement DNS filtering on all devices—whether in-office, remote, or mobile. Our RoundClock DNS Filtering Solution, powered by **Cisco Umbrella**, blocks access to malicious websites and phishing attempts, protecting employees from cyber threats wherever they work. ☐

10 **Device Compliance:** Ensure that devices accessing your network meet security standards, including necessary features and up-to-date software, protecting against potential threats. ☐

11 **Vulnerability Scanning & Security Audits:** Regular checks for weaknesses in your systems are essential to keeping safe. RoundClock Security Suite provides thorough scans and routine security assessments, with easy-to-understand reports and practical recommendations to fix any issues and strengthen your defences. ☐

12 **Safe Device Disposal:** Ensure all business devices are securely wiped and factory reset before selling, donating, or disposing of them to prevent any risk of data leakage. ☐

Prepare your Staff

13 **Cybersecurity Awareness Training:** Educate employees on the importance of cybersecurity, including how to recognise phishing emails, avoid suspicious links, and maintain secure habits online. ☐

14 **Incident Response & Business Continuity Plan:** Create a plan to manage cyber incidents, including how to isolate systems, notify key people, and recover quickly. ☐