Cyber Security Checklist for Small Businesses

TELECO
Integrating Technologies

Before your business falls prey to cyber threats, empower yourself with knowledge. Welcome to our Cybersecurity Assessment, a vital resource for securing your digital assets comprehensively. It's time to take proactive steps towards safeguarding your business. Begin by initiating a conversation with your IT provider today to assess your current cybersecurity posture.

□ Phishing Protection

Are phishing protection measures in place, such as email filtering to detect and quarantine suspicious emails?

Does the provider conduct regular phishing simulations to test employees' awareness and responsiveness?

□ Endpoint Security

Is antivirus and anti-malware software installed on all endpoints (computers, mobile devices)?

Are endpoints regularly updated and patched against security vulnerabilities?

□ Firewall & Intrusion Detection

Is there an active firewall with intrusion detection and prevention capabilities in place?

Are logs monitored for unusual or suspicious activities?

□ Access Control & Authentication

Is multi-factor authentication (MFA) implemented for critical systems and applications?

Are user access permissions reviewed and updated regularly based on the principle of least privilege?

□ Data Backup & Recovery

Is there a data backup and recovery plan in place, including offsite backups?

Are backup systems tested periodically to ensure data can be restored?

□ Incident Response Plan

Is there an incident response plan outlining steps to follow in case of a cybersecurity incident?

Have tabletop exercises or simulations been conducted to test the response plan?

□ Security Patch Management

Are security patches and updates regularly applied to operating systems and software?

Is there a process for quickly addressing critical security vulnerabilities?

□ Employee Training

Is cybersecurity awareness training provided to employees on an ongoing basis?

Are employees educated about social engineering tactics and how to recognize them?

□ Vendor & Third-Party Security

Is there a process for assessing and managing the cybersecurity posture of third-party vendors and suppliers?

□ Security Audits & Compliance

Are regular security audits and compliance assessments conducted?

Is the organization compliant with relevant industry standards (e.g., PCI DSS, HIPAA)?

□ Encryption & Data Protection

Is sensitive data encrypted both in transit and at rest?

Are encryption best practices followed for securing communications and storage?

□ Mobile Device Security

Are mobile devices used for work purposes protected with security policies and remote wipe capabilities?

Is mobile device security included in the overall cybersecurity strategy?

□ Monitoring & Threat Detection

Are there mechanisms in place to monitor network traffic and detect unusual or malicious activities?

Is there a process for responding to security incidents in real-time?

□ Regular Security Updates

Does the IT provider regularly communicate cybersecurity updates and recommendations to the business?

□ Disaster Recovery & Business Continuity

Is there a disaster recovery plan ensuring the business can continue operations in case of a cyber incident?

Are critical systems prioritized for recovery?

□ Employee Offboarding

Is there a process to revoke access for employees who leave the organization?

□ Cyber Insurance

Does the organization have cybersecurity insurance coverage in case of a breach?

□ Security Documentation

Are cybersecurity policies, procedures, and documentation kept up-to-date and easily accessible?

If you need assistance strengthening your cybersecurity defences or have questions regarding this checklist, talk to one of our local cybersecurity experts today. Your security is our priority

1218 Amber Drive • 807-345-2900 • 1-800-465-3933 • sales@teleco.ca • Teleco.ca