

SME CYBERSECURITY CHECKLIST

A Practical Guide for Small Business Security

Created by Jamola Cybersec Services Limited

INTRODUCTION

Cybersecurity is not just for large enterprises. Small and medium-sized businesses are increasingly targeted by cybercriminals because they often have weaker security controls. This checklist will help you identify and address the most critical security gaps in your business.

CHECKLIST

□ 1. Implement Multi-Factor Authentication (MFA)

- Enable MFA for all email accounts
- Use MFA for all cloud applications
- Require MFA for remote access

□ 2. Use Strong Password Policies

- Require passwords with at least 12 characters
- Enforce complexity (uppercase, lowercase, numbers, symbols)
- Implement password expiry policies (90 days recommended)
- Prohibit password reuse

□ 3. Keep Software Updated

- Enable automatic updates for operating systems
- Update all applications regularly
- Patch critical vulnerabilities within 48 hours

□ 4. Backup Your Data

- Follow the 3-2-1 backup rule:
- 3 copies of your data
- 2 different storage media
- 1 copy stored offsite
- Test backups monthly

□ 5. Train Your Employees

- Conduct security awareness training
- Run phishing simulations
- Train staff on reporting suspicious activity

□ 6. Use Antivirus and Endpoint Protection

- Install reputable antivirus software
- Ensure real-time protection is enabled
- Schedule regular scans

□ 7. Secure Your Network

- Use WPA3 or WPA2 encryption for Wi-Fi
- Change default router credentials
- Enable firewall protection

□ 8. Control Access to Information

- Apply the principle of least privilege
- Review user access regularly
- Remove access for departed employees

□ 9. Encrypt Sensitive Data

- Use encryption for data at rest
- Use encryption for data in transit
- Implement email encryption for sensitive communications

□ 10. Develop an Incident Response Plan

- Document response procedures
- Assign roles and responsibilities
- Test your plan annually

□ 11. Conduct Security Audits

- Schedule regular security assessments
- Use external auditors when possible
- Act on audit findings

□ 12. Review Third-Party Access

- Assess vendor security practices
- Review third-party access regularly
- Require NDAs and security clauses

EMERGENCY CONTACTS

Cybersecurity Contact: _____

IT Support: _____

Emergency Response: _____

ABOUT JAMOLA CYBERSEC SERVICES LIMITED

Jamola Cybersec Services Limited provides remote cybersecurity services to SMEs worldwide. We help businesses secure their systems, protect their data, and build resilient security programmes.

Contact: info@jamolacybersec.uk

Website: <https://jamolacybersec.uk>

© 2026 Jamola Cybersec Services Limited. All rights reserved.