Small Business Cybersecurity Checklist

2026 Edition — 25 Actionable Steps

Prepared by Forti365 | forti365.com

Forti365

This checklist covers the essential security controls every small and midsize business should have in place. Work through each section, check off completed items, and prioritize the gaps. Red items are critical — address those first.

Critical — do this week Important — do this month Good practice — plan for this quarter

Identity & Access Management

- [ ] **1. Enable MFA on all accounts**
  Email, banking, cloud, CRM — every account with business data. Use authenticator apps (Microsoft/Google Authenticator) or hardware keys (YubiKey) for admins. Blocks 99.9% of automated attacks.
- [ ] **2. Eliminate shared passwords and accounts**
  Every user gets their own credentials. Deploy a password manager company-wide (Bitwarden, 1Password). Minimum 14-character passwords with no reuse.
- [ ] **3. Review and remove ex-employee access**
  Audit Active Directory, M365, AWS, and all SaaS apps. Disable accounts immediately on departure. Check for lingering access keys, shared mailboxes, and delegated permissions.
- [ ] **4. Apply least-privilege access**
  Users should only access what they need for their role. Review admin accounts quarterly — most organizations have 3-5x more admins than necessary.

Email & Microsoft 365 Security

- [ ] **5. Configure SPF, DKIM, and DMARC**
  Prevents email spoofing and improves deliverability. Without these, attackers can send emails that appear to come from your domain.
- [ ] **6. Enable conditional access policies**
  Block sign-ins from unusual locations, require compliant devices, and enforce MFA for risky sign-ins. Available in M365 Business Premium and above.
- [ ] **7. Enable audit logging and alerts**
  Turn on unified audit log in M365. Set alerts for suspicious activities: impossible travel, mass file downloads, mailbox forwarding rules created.

- [ ] **8. Backup M365 data independently**
  Microsoft retention is not backup. Use a third-party solution (Veeam, Datto, Acronis) to back up Exchange, OneDrive, SharePoint, and Teams data.

Network & Firewall Security

- [ ] **9. Update firewall firmware and review rules**
  Outdated firmware = known vulnerabilities. Review rules quarterly — remove any "allow all" rules, close unused ports, and verify no default passwords remain.
- [ ] **10. Segment your network**
  Separate guest WiFi, IoT devices, servers, and workstations into different VLANs. A compromised printer should not be able to reach your file server.
- [ ] **11. Secure WiFi with WPA3 and separate SSIDs**
  Corporate WiFi on its own VLAN with device authentication. Guest WiFi isolated with bandwidth limits. Change default router/AP passwords.
- [ ] **12. Enable intrusion detection/prevention (IDS/IPS)**
  Most modern firewalls include IDS/IPS — make sure it is enabled and signatures are updated. Review alerts weekly for signs of probing or lateral movement.

Endpoint & Device Security

- [ ] **13. Deploy endpoint detection and response (EDR)**
  Traditional antivirus is not enough. Use EDR (Microsoft Defender for Business, SentinelOne, CrowdStrike) that detects behavioral threats, not just known signatures.
- [ ] **14. Enable automatic OS and software patching**
  60% of breaches exploit known vulnerabilities. Enable Windows Update, configure patch management for third-party apps (browsers, Adobe, Java). Patch within 14 days of release.
- [ ] **15. Encrypt all laptops and portable devices**
  Enable BitLocker (Windows) or FileVault (Mac) on every device. A lost unencrypted laptop is a data breach — with encryption, it is just a hardware loss.
- [ ] **16. Implement mobile device management (MDM)**
  If employees access company data on personal phones, require a PIN, enable remote wipe capability, and enforce app-level protections. Microsoft Intune is included in M365 Business Premium.

Cloud Security (AWS / Azure / SaaS)

- [ ] **17. Secure root/global admin accounts**

Lock down AWS root account and Azure Global Admin with hardware MFA. Never use them for daily operations. Create separate admin accounts with just enough permissions.

- [ ] **18. Enable cloud logging and monitoring**
  Turn on CloudTrail (AWS), Activity Log (Azure), or audit logs for all SaaS apps. You cannot detect what you do not log. Set up alerts for critical changes.

- [ ] **19. Review public access and sharing settings**
  Check S3 bucket policies, Azure Blob access, OneDrive/SharePoint sharing links. Block public access by default. Audit external sharing quarterly.

- [ ] **20. Enable encryption at rest and in transit**
  Ensure all stored data is encrypted (S3, RDS, EBS, Azure Storage). Force HTTPS everywhere. Use TLS 1.2+ for all connections.

Backup & Disaster Recovery

- [ ] **21. Implement 3-2-1 backup strategy**
  3 copies of data, 2 different media types, 1 offsite/cloud copy. Include at least one air-gapped or immutable backup that ransomware cannot reach.

- [ ] **22. Test restore procedures quarterly**
  A backup you have never tested is not a backup. Perform a full restore test at least quarterly. Document recovery time and verify data integrity.

People & Process

- [ ] **23. Conduct security awareness training**
  Train all employees to recognize phishing, social engineering, and suspicious links. Run simulated phishing tests monthly. Make reporting easy and non-punitive.

- [ ] **24. Document an incident response plan**
  Know who to call, how to isolate systems, and how to communicate when something goes wrong. A plan you have never practiced will fail under pressure.

- [ ] **25. Review cyber insurance coverage**
  Verify your policy covers ransomware, business interruption, and data breach costs. Many policies require specific controls (MFA, backups) — confirm you meet the requirements.

Need Help Implementing This Checklist?

Book a free 30-minute IT strategy session. We will review your results together and prioritize the gaps that matter most for your business.

forti365.com/book