Good Security

CHECKLIST WATERMARKED PDF

OPERATIONAL CHECKLIST

# NZ SME Security Checklist

20 essential security controls every New Zealand business should have in place. Work through each item to understand your current exposure and prioritise remediation.

Branded customer-ready document | Shareable with leadership teams | Generated 12 Mar 2026

## 20 essential controls every NZ business should have in place

**Good Security** · goodsecurity.co.nz · **hello@goodsecurity.co.nz**

> **How to use this checklist** Work through each control and mark it ✅ Done, ⚠️ Partial, or ❌ Not Done. Anything not fully done is a risk that deserves attention. Controls are ordered by impact — the top items address the most common attack vectors facing NZ businesses.

## SECTION 1: IDENTITY & ACCESS CONTROL

**1. Multi-factor authentication (MFA) on all email accounts** All staff email accounts — Microsoft 365, Google Workspace, or equivalent — require MFA. Email is the single highest-value target for attackers and the first control insurers ask about.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

**2. MFA on all cloud services and business applications** Every system staff access — accounting software, CRM, cloud storage, HR systems — requires MFA. A password alone is not sufficient protection for business systems in 2026.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

**3. Unique passwords managed through a business password manager** No shared passwords. No reused passwords across systems. A business password manager — Bitwarden, 1Password, or similar — is deployed and in active use.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**4. Privileged access is restricted** Global administrator and IT admin accounts are limited to the minimum number of staff who genuinely need them. Admin accounts are separate from day-to-day user accounts.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**5. Leavers are offboarded within 24 hours** There is a documented, followed process to revoke access when a staff member leaves. Accounts are disabled — not just password-changed.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

## SECTION 2: DEVICE SECURITY

**6. All devices have endpoint protection installed** Business-grade antivirus/EDR — Microsoft Defender for Business, Sophos, CrowdStrike, or equivalent — is installed and active on all computers used for work, including personally owned devices that access business systems.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**7. Operating systems are kept up to date** Windows, macOS, and mobile operating systems receive security updates promptly. Automatic updates are enabled or there is a defined patching schedule.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**8. Full-disk encryption is enabled on all laptops** BitLocker (Windows) or FileVault (Mac) is enabled on all laptops. This protects business data if a device is lost or stolen — a common incident for NZ businesses.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**9. Screen lock is enforced** All devices automatically lock after 5–10 minutes of inactivity and require a PIN, password, or biometric to unlock.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**10. Business data on personal devices is governed** If staff access business email or files on personal phones or computers, there is a policy setting minimum security requirements and acceptable use.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

## SECTION 3: EMAIL & PHISHING DEFENCE

**11. Email authentication records are configured (SPF, DKIM, DMARC)** Your domain has SPF, DKIM, and DMARC DNS records configured. These make it significantly harder for attackers to send email that appears to be from your business — a prerequisite for most BEC attacks.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

**12. Anti-phishing filtering is active on email** Microsoft Defender for Office 365, Google Workspace Advanced Protection, or equivalent anti-phishing controls are active and configured.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

**13. Staff can recognise and report phishing** All staff have completed security awareness training in the last 12 months covering how to identify phishing emails and what to do if they receive one.

☐ Status: ✅ / ⚠️ / ❌ Date of last training: _____

## SECTION 4: DATA & BACKUPS

**14. Critical business data is backed up at least daily** Backups run at minimum daily for critical data. Backups are stored separately from the systems they protect — offsite, cloud with deletion protection, or air-gapped.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

**15. Backups have been successfully tested** A restore has been tested in the last 12 months and confirmed successful. An untested backup is not a backup — it is an assumption.

☐ Status: ✅ / ⚠️ / ❌ Date of last restore test: _____

**16. Sensitive data is classified and controlled** Your business knows what personal or confidential information it holds, where it is stored, and who has access to it. This is a foundational requirement of the Privacy Act 2020.

☐ Status: ✅ / ⚠️ / ❌ Notes: _____

## SECTION 5: NETWORK & REMOTE ACCESS

**17. Business Wi-Fi is separate from guest Wi-Fi** If your office has Wi-Fi, guests and personal devices connect to a separate network. Business systems are not accessible from the guest network.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**18. Remote access uses secure methods** Staff accessing business systems remotely use VPN with MFA, or cloud-based systems with MFA enforced. Remote Desktop Protocol (RDP) is not exposed directly to the internet.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

## SECTION 6: GOVERNANCE & RESPONSE

**19. There is a documented plan for responding to a cyber incident** Even a one-page document — who to call, what to isolate, how to notify affected parties — is significantly better than nothing. A ransomware attack is not the time to figure out your response process.

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

**20. Privacy Act 2020 obligations are understood by key staff** Key staff understand when a privacy breach must be reported to the Privacy Commissioner and to affected individuals. The threshold is "likely to cause serious harm."

□ Status: ✅ / ⚠️ / ❌ Notes: _____

---

## YOUR SCORE

| STATUS | COUNT |
|---|---|
| ✅ Done | |
| ⚠️ Partial | |
| ❌ Not Done | |

**16–20 Done:** Strong foundation. A full security baseline assessment will identify what to tackle next and help you evidence your posture for insurance or compliance purposes.

**10–15 Done:** Moderate risk exposure. Prioritise MFA (controls 1–2), backups (controls 14–15), and patching (control 7) first — these address the most common attack vectors against NZ SMEs.

**Under 10 Done:** High risk. Most of these controls are low-cost or already included in the Microsoft 365 or Google Workspace licences you likely pay for — they need to be turned on and configured correctly. Contact Good Security for a free health check.

## WHAT TO DO NEXT

Controls marked Partial or Not Done represent real, measurable risk. The good news: the majority are configuration tasks on software you already licence, not new purchases.

If you want help prioritising or implementing these controls, Good Security offers a free 30-minute security health check for NZ businesses.

**Book a health check at https://goodsecurity.co.nz/health-check**