

Security Basics Pack



A do-this-first pack for NZ SMEs: identity baseline, backup confidence, invoice fraud controls, and templates.

Last updated: 2026-02-20 · Region: Taranaki focus, NZ-wide scope

Security Basics Pack

A do-this-first pack for NZ SMEs. If you do nothing else, get these right.

1) Identity baseline (MFA + admin hygiene)

- ✓ MFA enforced for all users (no exceptions without approval).
- ✓ Separate admin accounts for privileged roles.
- ✓ At least 2 break-glass accounts documented and tested quarterly.
- ✓ Conditional Access baselines: block risky sign-ins and legacy auth.
- ✓ Service accounts tracked with owners; shared accounts removed.

2) Email and invoice fraud controls

- ✓ DMARC/SPF/DKIM configured and monitored.
- ✓ External sender tagging enabled.
- ✓ Payment change procedure: verify bank changes out-of-band (phone call).
- ✓ Shared mailbox access reviewed quarterly.

3) Endpoint basics (patching + protection)

- ✓ Automatic updates on and monitored (OS + browsers).
- ✓ Endpoint protection/EDR deployed where licensed and tuned.
- ✓ Local admin rights removed (use controlled elevation).
- ✓ Device encryption enabled on laptops.

4) Backup confidence

- ✓ Critical systems identified (what must be restored first).
- ✓ Backups monitored daily; failures actioned.
- ✓ Restore test performed at least quarterly and recorded.
- ✓ Backup credentials protected (vault + MFA).

5) Vendor access and offboarding

- ✓ Vendor access register maintained (who has access, why, expiry).
- ✓ Offboarding checklist executed same day for leavers.
- ✓ Shared secrets rotated when staff or vendors change.

Templates (copy/paste)

A) Vendor Access Register

| Vendor | System | Access type | Account | Owner | Expiry/re view | Notes |
|--------|--------|-------------|---------|-------|----------------|-------|
| | | | | | | |
| | | | | | | |

B) Offboarding checklist

- Disable account and revoke sessions.
- Remove from groups and shared mailbox access.
- Rotate shared passwords/service credentials if required.
- Recover device and wipe if needed.
- Forward email or set auto-reply (if approved).
- Update access register and close the ticket.

C) Backup restore test log

| Date | System | Restore type | Result | Time to restore | Follow-up actions |
|------|--------|--------------|--------|-----------------|-------------------|
| | | | | | |
| | | | | | |

If you do only 3 things this week

- Enforce MFA for everyone and remove legacy authentication.
- Run one restore test and write down the result.
- Implement payment-change verification (invoice fraud control).

Book your free consultation today

hello@virtusgroup.biz

virtusgroup.co.nz

0800 847 887 (VIRTUS)