# SMB Device Security Starter Checklist

Apple, Microsoft, endpoint protection, and network basics for growing businesses

New Gauge Digital

For Australian SMBs and trades building a reliable device and security foundation. Tick what you already have — gaps become a clear project or managed service conversation.

## 1. Roles & device mix

- [ ] Every role has a defined device type (MacBook Neo for standard seats, Air/Pro for power users, iPad for field).
- [ ] Company-owned vs BYOD rules are written and understood.
- [ ] New-hire device provisioning has a repeatable process.
- [ ] Lost, stolen, and offboarding steps are documented.

## 2. Apple Business Manager & management

- [ ] Apple Business Manager is set up for the organisation.
- [ ] Automated Device Enrolment is used for company Macs and iPads.
- [ ] MDM is in place (Jamf Now for simple fleets, Jamf Pro as you grow).
- [ ] Apps and security policies are managed centrally — not by personal Apple IDs alone.

## 3. Identity & Microsoft 365

- [ ] Staff use corporate identity (Microsoft 365 / Entra ID) for work apps.
- [ ] MFA is enforced for email and admin access.
- [ ] Shared mailboxes and external sharing rules are controlled.
- [ ] Windows devices (if any) are managed alongside Apple — not as a separate mess.

## 4. Endpoint protection & response (Sophos)

- [ ] Next-gen endpoint protection is installed on work devices.
- [ ] You have a plan for after-hours threats (e.g. Sophos MDR).
- [ ] Alerts have an owner — not an ignored inbox.
- [ ] Security tools are managed from one console where possible (Sophos Central).

## 5. Network & access (UniFi)

- [ ] Office Wi-Fi is designed for staff density and guest separation.
- [ ] Critical gear is on reliable switching and power where needed.
- [ ] VPN or secure remote access is defined for hybrid work.
- [ ] Multi-site / trades locations have a consistent network approach.

## 6. Insurance & compliance readiness

- [ ] You know what your cyber insurer asks for (MFA, backups, endpoint, logging).
- [ ] Backups of critical data are tested, not only configured.
- [ ] Admin accounts are limited and reviewed.
- [ ] A short incident contact list exists (who to call first).

## 7. Operate or hand over

- [ ] Someone owns day-to-day device and security operations.
- [ ] You have either internal capacity or a managed partner for MDR and devices.
- [ ] Documentation exists so growth does not depend on one person's memory.

## Next step

Bring this checklist to a discovery call. New Gauge Digital delivers Apple setup, Jamf, Sophos Central, UniFi, and managed device security for growing Australian businesses — quote-based, no public price list.

**Book a discovery call → newgaugedigital.com.au/pages/contact**