

Identity and email

Assign every item to a person. Write Y (yes), N (no) or ? (not sure) inside each box. Treat ? as a follow-up, not a reason to guess. Ask the person who manages your Microsoft 365 business account for evidence.

BUSINESS _____	MICROSOFT 365 OWNER _____
SECURITY SETTINGS MANAGED BY _____	FINANCE PROCESS OWNER _____
EVIDENCE FOLDER _____	REVIEW DATE _____

01

PRIORITISED FIRST STEP

Enforce multi-factor authentication for every account.

Start with owners, finance staff and administrators, then cover every user. Prefer an authenticator app, passkey or security key over text messages where practical.

1

Accounts and administrators

- ☐ Every user has multi-factor authentication and knows to deny and report unexpected prompts.
- ☐ Administrators use a separate account for system changes, not their everyday email account.
- ☐ Administrator roles are limited, individually assigned and reviewed regularly.
- ☐ Each administrator account has business-controlled recovery methods and a tested recovery path.
- ☐ Former staff, contractors, test accounts and unused users are blocked or removed promptly.

MICROSOFT 365 OWNER _____

ADMIN / IDENTITY EVIDENCE _____

2

Email and payment protection

- ☐ Spam and phishing settings are reviewed, with alerts going to someone who will act.
- ☐ Email authenticity records are configured and monitored so receiving systems can verify messages from the business domain. The technical names are SPF, DKIM and DMARC.
- ☐ Unexpected forwarding rules and sent messages are investigated.
- ☐ Changed bank details are confirmed by calling a known number, outside the email thread.

EMAIL OWNER _____

EMAIL SETTINGS / DOMAIN EVIDENCE _____

Protect the work

CHECKLIST · 02

3 Sharing and departures

- ☐ Important OneDrive, SharePoint and Teams access has a named business owner.
- ☐ Old public links and access held by former staff, contractors or suppliers are removed.
- ☐ External links use expiry dates where suitable.
- ☐ Before an account is deleted, required email, OneDrive files and records are transferred.

DATA OWNER

SHARING REVIEW

4 Devices and recovery

- ☐ Work devices require screen locks, current updates and managed device protection.
- ☐ The business can remove company data from a lost or stolen device.
- ☐ Email, OneDrive, SharePoint and Teams recovery requirements are documented.
- ☐ A separate Microsoft 365 backup is protected from normal user accounts and a restore is tested.

DEVICE / BACKUP
OWNERRESTORE DATE /
RESULT

5 Alerts, staff and licences

- ☐ Unusual sign-ins are reviewed using the device, time and user context, not location alone.
- ☐ Staff receive short, regular examples of fake Microsoft sign-in pages, attachments and approval prompts.
- ☐ There is one simple reporting path and staff can ask before clicking without blame.
- ☐ Licences, enabled security features and user needs are reviewed together before licences or accounts are removed.

REVIEW OWNER

REVIEW RECORD

REVIEW OUTCOME

CRITICAL GAPS

ACTION OWNER

TARGET DATE

A SECOND SET OF EYES

Turn unknowns into owners.

JCPIT can review account, email, sharing, device and recovery settings. You receive a prioritised record of what works, what needs action and who owns it.

jcpit.com.au/free-security-check/
(03) 9021 0890

Recommended review order: multi-factor authentication, administrators, departing staff, recovery, then email, sharing, devices and training. Store the completed checklist securely. Do not record passwords, authentication codes, full bank details or unnecessary personal information.