USE IT MATE

SECURE EMPLOYEE OFFBOARDING CHECKLIST

A simple, practical guide to protect your business data when staff leave.

- Prevent data theft and access issues
- Avoid surprise security risks
- Reduce downtime during staff changes

Printing tip:
For best results, print in A4, black & white, single-sided.
This checklist is designed to be used during employee exit procedures.

Store the completed checklist with employee records.

Queensland-based • Remote-first • Managed IT for businesses

STEP 1: IMMEDIATE ACCOUNT LOCKDOWN (DO THIS FIRST)

As soon as an employee leaves, these steps prevent access to company systems and data.

Checklist:

□ Disable sign-in to Microsoft 365 user account
□ Reset account password to a secure, random password
□ Force sign-out from all active sessions and devices
□ Revoke active refresh tokens (prevents silent re-login)
□ Disable access to company VPN or remote access tools
□ Remove user from all security groups and admin roles

Important:
Blocking sign-in alone is not enough. Active sessions and mobile devices must be forcibly signed out to fully cut access.

Tip: These steps should be completed immediately to prevent data access after termination.

STEP 2: DATA & EMAIL PRESERVATION

Retain business data without keeping the employee account active.

Checklist:

□ Convert mailbox to shared mailbox (retain email history)
□ Remove Microsoft 365 license to stop ongoing charges
□ Review and remove inbox rules or auto-forwarding
□ Transfer ownership of OneDrive files to a manager
□ Review SharePoint and Teams permissions
□ Remove user from shared mailboxes and calendars

Note: Inbox rules and auto-forwarding are a common data leak risk and should always be reviewed.

STEP 3: THIRD-PARTY & SHADOW IT ACCESS

Employees often retain access to systems outside Microsoft 365.

Checklist:

□ Accounting systems (Xero, MYOB, payroll)
□ CRM and customer databases
□ Design tools (Canva, Adobe, Figma)
□ Project tools (Trello, Asana, ClickUp)
□ Messaging tools (Slack, Zoom, Teams guest access)
□ Password managers and shared credentials
□ Marketing or social media accounts
□ Backup systems or admin portals

If unsure, reset shared passwords immediately.

STEP 4: FINAL SECURITY CHECK

Retain business data without keeping the employee account active.

Checklist:

□ Review recent login activity for unusual access
□ Check for recent mass downloads or deletions
□ Confirm no external sharing links remain active
□ Verify no admin access is still assigned

STEP 3: COMPANY ASSET RETURN CONFIRMATION

Confirm all business equipment and access has been returned or revoked.

Employee Name: _____

Role: _____

Last Working Day: _____

Asset Checklist:

□ Laptop / Computer
□ Mobile phone
□ Security keys / MFA devices
□ ID cards / access passes
□ Other equipment: _____

I confirm all company property has been returned and I no longer have access to business systems or data.

Employee Signature: _____

Manager Signature: _____

Date: _____

This checklist is provided as a general guide. For full implementation or assistance, professional IT support may be required.