USE IT MATE

SECURE EMPLOYEE OFFBOARDING CHECKLIST

Standard Operating Procedure for protecting business data when staff leave.

Author: Jasson Borgueta, Technical Lead — Use IT Mate (Bundaberg & Wide Bay)

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

Store the completed checklist with employee records.

PHASE 1: DO THIS IMMEDIATELY (Day 0)

Complete these steps immediately upon termination.

□ Physically collect laptops, mobiles, and MFA hardware tokens.

□ Collect Office Keys, Swipe Cards, and Alarm Fobs.

□ Reset Microsoft 365 Password (then revoke sessions below)

□ Critical: Revoke all active "Session Tokens" (Forces mobile logout).

□ Block user sign-in in Microsoft Entra ID (formerly Azure AD)

□ Remove device from Bank Account "Trusted Device" list.

□ Reset/disable MFA methods (Authenticator, SMS, phone) and remove recovery email/phone

□ Revoke app passwords (if used)

□ Change Building Alarm Code.

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.

PHASE 2: CLEAN UP DEVICES (Day 1)

□ Verify BitLocker Encryption is active (prevent data recovery).

□ Initiate "Remote Wipe" or "Factory Reset" on company laptop.

□ Perform "Selective Wipe" on personal BYOD phones (removes corporate data only).

□ Rotate office Wi-Fi password (if using a shared password/PSK)

□ Check for unauthorised email forwarding or large attachments (Sent Items / Outbox)

□ Check Inbox Rules and Auto-forwarding settings and mailbox delegates

□ Check delegates/shared mailbox access granted to the user

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

PHASE 3: COMPLIANCE & ARCHIVE (Week 1)

□ Revoke access to industry portals / line-of-business apps (e.g., AFG/Connective/Xplan)

□ Remove Admin rights from Facebook/LinkedIn pages.

□ Convert email to "Shared Mailbox" for manager access.

□ Apply "Legal Hold" or Retention Policy to email archives.

□ Transfer ownership of OneDrive (and preserve data)

□ Remove user from Teams / M365 Groups and reassign ownership where needed

If unsure, reset shared passwords immediately.

PHASE 4: FINAL SECURITY CHECK

Ensure all loose ends are tied up.

□ Review recent login activity for unusual access

□ Check for recent mass downloads or deletions

□ Verify no admin access is still assigned

□ Remove/disable any external sharing links (SharePoint/OneDrive/Drive)

□ Remove from admin roles / privileged groups

□ Review enterprise app / OAuth app access and revoke where applicable

Sounds like a lot of work?

We can automate most of this.
We configure your systems to "Remote Wipe"
and "Auto-Lock" devices instantly, so you never
have to worry about rogue data again.

PHASE 5: 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.