

IT Offboarding Verification Checklist

A laptop back and an inbox disabled isn't finished offboarding. Verify each item below, log who owns it and what proved it, before you consider access closed.

Employee: _____ Departure date & cutoff time: _____ Coordinator: _____

1 Email Forwarding and Inbox Rules

- ☐ Mailbox reviewed for forwarding/inbox rules at the same cutoff as the account actions below (does not delay them)
- ☐ Unauthorized rules captured as evidence, then removed; approved continuity rules left in place

Owner: _____ Evidence: _____

2 Account, Sessions, and MFA

- ☐ Account sign-in disabled
- ☐ Active sessions/refresh tokens revoked (separate step; confirm it took effect on services, not just the admin console)
- ☐ MFA methods (Authenticator app, phone, etc.) removed as part of cleanup (not an access-blocking control on its own; not a substitute for disable/revoke)
- ☐ App passwords and third-party app consent grants reviewed and revoked
- ☐ Access confirmed cut off on personal devices too (identity-level control); anything cached on that device flagged separately, removable only if app protection/device management was already configured for that app

Owner: _____ Evidence: _____

3 SaaS Licenses and Subscriptions

- ☐ Full inventory of tools/subscriptions this person had access to, including any signed up for outside normal IT provisioning
- ☐ Each account explicitly disabled/deprovisioned and any app-issued sessions or tokens revoked; access verified gone, not just license freed
- ☐ Business records exported or transferred before the license is removed or account deleted, where retention matters (does not delay disable/revoke above)

Owner: _____ Evidence: _____

4 Wi-Fi, Physical Access, and Assets

- ☐ Individual Wi-Fi credential or keycard identity revoked
- ☐ Shared Wi-Fi password or shared keycard code known to this person rotated; if not same-day, named owner and deadline set, with interim restrictions until then
- ☐ Company devices, keys, badge, and other physical assets collected and inventoried

Owner: _____ Evidence: _____

Before You Close This Out

- ☐ Revoking access does not delete data already downloaded, exported, or synced before offboarding began. Secure those records first if they matter.
- ☐ If a personal (BYOD) device was used for work, remove company data/accounts through whatever app protection/device management policy was already configured for that app. Not a full device wipe, and not guaranteed for data downloaded outside a managed app.
- ☐ HR and IT should confirm the departure date and cutoff time together so offboarding starts on schedule, not sometime that week.