

Hands-on Offboarding Checklist

15-minute containment

- ☐ Suspend identity: Block sign-in; revoke refresh tokens.
- ☐ Kill admin: Remove from all admin roles & privileged groups.
- ☐ Nuke delegation: Remove mailbox send-as/on-behalf; shared mailbox access.
- ☐ Stop exfil: Disable external forwarding; delete inbox rules; pause OAuth app consents.
- ☐ Drop sessions: Terminate VPN/SSO sessions; revoke SSH/RDP keys.
- ☐ Freeze devices: Lock/isolate managed devices via MDM; consider remote wipe.
- ☐ Snapshot evidence: Save auth/email/share/admin logs; record timestamps.
- ☐ Document chain: Note who did what/when for chain of custody.

Same-day cleanup

- ☐ Rotate shared secrets: vault passwords, API tokens, app passwords.
- ☐ Remove everywhere: all groups, DLs, Teams/Slack, file shares, wikis, repos.
- ☐ Reassign ownership: docs, projects, calendars, repositories.
- ☐ Comms: set Out-of-Office; (optional) route mail to monitored mailbox (time-boxed).
- ☐ Facilities: collect badges/keys; change door codes/Wi-Fi PSKs if used.
- ☐ HR/Legal: confirm device return; legal hold if dispute.
- ☐ Device intake: image if needed → wipe/re-provision.
- ☐ Backups: verify user data in backup scope.

Next 7–14 days

- ☐ Access recert: remove standing admin; move to JIT elevation.
- ☐ Review + update: runbook/policy, lessons learned.
- ☐ Logging: centralize; retain ≥ 90 days; add alerts for risky patterns.
- ☐ Hygiene: MFA everywhere (number-match/FIDO); rotate shared keys quarterly.