Microsoft 365 offboarding checklist

Secure access, protect business information and document the handover.

Employee / identifier: _____ Ticket: _____

Cutoff date, time and time zone: _____ IT owner: _____

Manager / HR contact: _____ Review date: _____

1 Prepare and approve

- [ ] Verify the leaver, cutoff, time zone, HR contact and accountable IT owner.
- [ ] Identify licences, admin roles, devices, applications, groups and critical dependencies.
- [ ] Agree mailbox and file access, named recipients, purpose, review dates and retention or legal holds.
- [ ] Record the approver for each decision. Secure access at the cutoff even if handover details remain open.

2 End access at the cutoff

- [ ] Block sign-in in Microsoft 365 and follow the source-directory process for hybrid identities.
- [ ] Revoke Microsoft Entra sign-in sessions and ask application owners to revoke independent sessions.
- [ ] Remove privileged roles, VPN and third-party access; rotate shared secrets and recovery methods.
- [ ] Verify the block and record exceptions. Tokens, offline devices and cached data may persist.

Preserve, transfer and verify

Complete these steps before removing licences or deleting the identity.

3 Mailbox and OneDrive

- [ ] Confirm preservation and hold requirements. Approve mailbox delegation, forwarding or automatic reply.
- [ ] If a shared mailbox is needed, convert it before licence removal; test named delegate access.
- [ ] Keep the associated account blocked and in place while it anchors a shared mailbox or forwarding.
- [ ] Check mailbox size, archive and hold licensing requirements before removing an Exchange licence.
- [ ] Give an approved successor limited OneDrive access. Transfer business files to a suitable shared location.
- [ ] Verify sample files, permissions, links, version history and the new owner; record outstanding items.

4 Ownership and devices

- [ ] Assign owners for Teams, groups, SharePoint sites, forms, flows, apps and other critical services.
- [ ] Test important automations, connections and credentials with the relevant application owner.
- [ ] Reconcile laptops, phones, keys and passes. Approve the scope before any wipe or selective removal.
- [ ] Check wipe completion; an offline device may retain local data. Escalate overdue returns or failures.

5 Licence and account decisions

- [ ] Check each affected workload, hold, retention and billing dependency before removing a licence.
- [ ] Delete the identity only after approval and after confirming it is not needed for mailbox or forwarding.
- [ ] Record the exact action and schedule follow-up for temporary access, retention and unresolved devices.

Record the evidence

Keep this record restricted and follow your organisation's retention policy.

Decision and business purpose

Approver and approval date

System, action, target and administrator

Action time and time zone

Verification or log reference

Exceptions, owner and next deadline

Retention / hold decision and review date

Licence and account deletion decision

Retention is not a backup

OneDrive deletion, unlicensed storage, holds and billing follow different rules. Confirm your tenant settings and current Microsoft guidance; test your backup and restoration process.

Read the full guide and source links

Technical guidance checked 5 November 2026. Confirm current settings before acting.