Identefi

CHECKLIST

Microsoft 365 Onboarding & Offboarding Checklists

The identity steps for every joiner, mover and leaver in Microsoft 365 and Entra ID, in the order they should happen.

How to use this

Assign a named owner for each stage, tick items as they are completed, and keep the completed copy as your record. Items marked ADMIN need a Microsoft 365 administrator.

Part 1: Onboarding

BEFORE THE START DATE

- [ ] Get written approval from the hiring manager or program lead (name, role, start date, and end date if a volunteer or contractor)
- [ ] Decide the access the role needs, based on a role template or a comparable current employee, not a copy of a colleague's full access
- [ ] Create the account using your standard naming convention ADMIN
- [ ] Assign licenses through a group, not by hand, so removal is automatic
- [ ] Add the user to role-based security groups, Teams and shared mailboxes. Do not grant access to individual files or folders directly
- [ ] Do not grant any administrator role. Admin access is a separate request with its own approval
- [ ] Prepare the device and enroll it in device management before it reaches the user
- [ ] Deliver the first sign-in details through a channel other than the one the account uses (a phone call or in person). Prefer a Temporary Access Pass over a shared password

DAY ONE

- [ ] User signs in and registers multifactor authentication (MFA) with an authenticator app
- [ ] User registers for self-service password reset
- [ ] Confirm Conditional Access and MFA policies apply to the new account
- [ ] User acknowledges the acceptable use and data handling policies
- [ ] Confirm the user can reach only what the role needs. Test one sensitive location they should not reach

WITHIN 30 DAYS

- [ ] Manager confirms access is correct and nothing is missing
- [ ] Remove any temporary or "just in case" access added during the first weeks
- [ ] Record the completed checklist

Part 2: Role change (mover)

People who change roles keep old access unless someone removes it. This is the step most organizations skip.

- [ ] Manager and IT agree the new access set
- [ ] Add the groups and permissions the new role needs
- [ ] Remove groups, shared mailboxes, Teams and SharePoint access that belonged to the old role
- [ ] Remove any administrator role that the new role does not need
- [ ] Record what changed and who approved it

Part 3: Offboarding

> Do the first block at the moment of departure, not at the end of the day or the following week. For involuntary departures, agree the exact time with HR in advance.

AT THE TIME OF DEPARTURE

- [ ] Confirm the departure date and time with HR and the manager
- [ ] Block sign-in **ADMIN**
- [ ] Revoke all active sessions **ADMIN**. Blocking sign-in alone does not end sessions that are already open, and issued tokens can stay valid for a period
- [ ] Reset the password **ADMIN**
- [ ] Remove registered MFA methods and sign-in devices **ADMIN**
- [ ] Remove any administrator role assignments **ADMIN**

SAME DAY

- [ ] Check the mailbox for forwarding and inbox rules, especially any that send mail to an outside address. Remove them
- [ ] Set an automatic reply that points senders to a named contact
- [ ] Give the manager access to the mailbox, or convert it to a shared mailbox. A shared mailbox under the storage limit does not need a license; check your own size before relying on this
- [ ] Give the manager access to the user's OneDrive files, and move what must be kept to a team location
- [ ] Remove the user from groups, Teams, distribution lists and shared mailboxes
- [ ] Reassign anything the user owned: groups, Teams, SharePoint sites, automations, applications
- [ ] Retire, wipe or collect the user's devices, including a personal phone if company data is on it

WITHIN ONE WEEK

- [ ] Remove the user from every other system that holds company data (donor or case management, accounting, HR, finance, password manager, remote access, and any app that does not sign in with Microsoft accounts)
- [ ] Review and revoke any third-party application permissions the user granted to company data
- [ ] Check for any legal hold or records retention requirement before data is removed
- [ ] Remove the license only after the mailbox and files are handled

AFTER THE RETENTION PERIOD

- [ ] Delete the account at the end of the retention period you have set. Deleted accounts can usually be restored for a limited time; confirm the window in your tenant
- [ ] Record the completed checklist, including date, time and who did each step

Part 4: Volunteers, contractors, board members and guests

- [ ] Give every non-employee account an end date when it is created
- [ ] Use guest access, not full accounts, where the person only needs to share files or join meetings
- [ ] Review all guest and non-employee accounts at least every quarter and remove any that have no sponsor or no recent use
- [ ] Run the offboarding checklist for them as well. Volunteers and board members are the accounts most often left active

Common gaps

- Offboarding starts days after the person has left
- Account disabled, but sessions, devices and app permissions still active
- Mailbox forwarding rules left in place
- Former staff still in shared mailboxes, Teams or distribution lists
- Admin roles never removed from people who changed jobs
- Volunteer and contractor accounts with no end date

Record

Employee / account _____ Completed by _____ Date _____

Want this running without the manual work? Identefi manages onboarding, offboarding and access reviews for Microsoft 365 organizations. **felipe@identefi.com** · identefi.com

General guidance for Microsoft 365 and Entra ID. Adapt it to your tenant's configuration, licensing and legal obligations. © Voss Technology Group LLC dba Identefi.