

CHECKLIST · TOMORIS TOOLBOX

IT Offboarding: Checklist for Departing Employees

Close out accounts, devices, data, and permissions in an orderly way, based on BSI IT-Grundschutz and with the steps for Microsoft 365

UPDATED

Oct 25, 2026

LENGTH

PDF, 8 pages

ONLINE

tomoris.com/en/downloads/it-offboarding-checkliste

AT A GLANCE

1 h

default validity of a Microsoft Entra ID access token

30 days

a deleted account remains recoverable

50 GB

shared mailbox without its own license

WHO IT IS FOR

- HR and people managers who support departures
- IT management and administrators of Microsoft 365 and Microsoft Entra ID
- Managers who organize handover, succession, and deputies

WHAT THIS COVERS

When employees leave the company, accounts, shares, and devices often remain that nobody keeps track of anymore. This checklist organizes the departure into three phases: before the last working day, on the last day, and afterward. It is based on requirements ORP.2.A2 and ORP.4.A2 of the BSI IT-Grundschutz Compendium. For Microsoft 365, it lists the steps and retention periods from Microsoft's documentation, so that no access remains open and no data is lost.

This checklist is a TOMORIS recommendation and does not replace advice on employment or data protection law. Names, steps, and retention periods in Microsoft 365 may change; Microsoft's current documentation is authoritative.

CONTENTS

01	What Must Be Defined for a Departure	2
02	The Process at a Glance	3
03	Before the Last Working Day	3
04	On the Last Working Day: End Access	4
05	After the Departure: Mailbox, OneDrive, and License	5
06	Special Case: Departure with Immediate Effect	6
07	Who Does What	7
08	Sources	7

01 —

What Must Be Defined for a Departure

The requirements of the BSI IT-Grundschutz Compendium for departing employees and for permissions.

The BSI IT-Grundschutz Compendium (2023 edition) covers departures in basic requirement ORP.2.A2 "Regulated procedure when employees leave." Supervisors and IT operations are responsible. Among other things, it requires:

- Successors are briefed in good time. If a direct handover is not possible, the departing employees document their tasks in detail.
- All documents, keys, and devices received in the course of the work, as well as ID badges and access authorizations, are collected.
- Before they leave, departing employees are reminded once more of their confidentiality obligations.
- Emergency plans and other procedures are updated, and all affected units, such as the IT department or security staff, are informed.

- There should be a checklist for the tasks involved, and a designated contact person in the HR department should accompany the departure.

For accounts and permissions, ORP.4.A2 applies: when personnel change, user IDs and permissions that are no longer needed must be removed. Under ORP.4.A3, the existing IDs, groups, and permission profiles are documented. This documentation is the basis for not overlooking anything during a departure.

The order and phases in this document are a TOMORIS recommendation. Your own policies and contracts are binding; the retention periods in Microsoft 365 come from Microsoft's documentation (for the date, see Sources).

02 —

The Process at a Glance

Three phases from learning of the departure to deleting the account.

Departure in phases (phases as a recommendation, retention periods according to Microsoft Learn)



Before

Plan the handover

Record tasks, data, accounts, and devices, brief successors and deputies, and decide how to handle the mailbox and OneDrive.



Last day

End access

Reset the password, block sign-in, revoke sessions, and collect devices, keys, and ID badges.



After

Hand over data

Convert or forward the mailbox, take over OneDrive content, remove the license, and remove permissions on shared resources.



Completion

Delete the account

Delete the account as soon as it is no longer needed for a shared mailbox or forwarding. It then remains recoverable for 30 days.

03 —

Before the Last Working Day

Handover, deputies, and a complete list of all access before time pressure sets in.

- ☐ A successor or deputy is named and briefed; where no direct handover is possible, the tasks are documented (ORP.2.A2, ORP.2.A3).
- ☐ All of the person's accounts are recorded: Microsoft 365 and Entra ID, local sign-in, business applications, VPN, cloud services, and supplier portals (based on the documentation under ORP.4.A3).
- ☐ Elevated permissions are known: administrative roles, permissions on other people's mailboxes, and ownership of Teams, groups, and SharePoint sites.
- ☐ Shared credentials known to the person are listed so they can be changed after the departure.

- ☐ Business data is stored in the designated shared storage and not only locally or in the personal OneDrive.
- ☐ A decision has been made for the mailbox: conversion to a shared mailbox or forwarding to a colleague.
- ☐ It is defined who takes over the OneDrive content. The person's manager is entered in Microsoft Entra ID; by default, the manager gets access when the account is deleted.
- ☐ Issued devices, security keys, keys, ID badges, and access media are on a list to check off.
- ☐ Emergency plans, contact lists, and on-call schedules are updated (ORP.2.A2).
- ☐ Affected units such as IT, reception, facility management, and external service providers know the departure date (ORP.2.A2).

04 —

On the Last Working Day: End Access

Reset the password, block sign-in, revoke sessions, and collect devices and access media.

1 Reset the password and sign out

In the Microsoft 365 admin center, reset the password and sign the person out of all sessions. According to Microsoft, resetting the password prevents sign-in immediately, whereas blocking sign-in can take up to 24 hours. An access token remains valid for up to one hour.

2 Block sign-in and revoke sessions

Block sign-in, which means turning off "Account enabled" in the Microsoft Entra admin center, and then select "Revoke sessions." The person then no longer receives new tokens for any application connected to Entra ID.

3 Don't forget on-premises Active Directory

If accounts are synchronized from an on-premises Active Directory, disable the account there as well and reset the password. Microsoft recommends resetting it twice to reduce the risk of pass-the-hash attacks; if the account is definitely not compromised, once is enough.

4 Wipe and block mobile devices

For smartphones used for work, remotely wipe the company data and block access in the Exchange admin center, or via Intune if they are managed with Intune. A wipe only takes effect when the device is online; while offline, locally stored data remains accessible.

5 Collect devices, keys, and ID badges

Take back the notebook, smartphone, security keys, keys, ID badges, and access authorizations, and check them off on the list (ORP.2.A2). Block access authorizations in the locking or access control system.

6

Applications outside Entra ID

Block applications with their own sign-in or their own sessions individually. Microsoft points out that Entra ID cannot revoke session tokens issued by applications; automatic deprovisioning closes this gap where the application supports it.

7

Change shared credentials

Change the passwords of shared accounts and access credentials that the person knew. The list from the preparation serves as a template.

Before saying goodbye, remind the person once more of existing confidentiality obligations (ORP.2.A2).

05

After the Departure: Mailbox, OneDrive, and License

What Microsoft 365 does with the mailbox, OneDrive, and account, and which retention periods apply.

Behavior and retention periods in Microsoft 365 (according to Microsoft Learn, accessed October 25, 2026)

TOPIC	WHAT APPLIES
Shared mailbox	The conversion keeps all email and the calendar. Without a license up to 50 GB; above that, the mailbox needs a license. The account must not be deleted for this.
Forwarding	Forwards only new email to the successor. The account and mailbox must remain in place; without a license, this is only possible via a shared mailbox with forwarding.
Remove license	A regular user mailbox is disconnected immediately and is no longer accessible; after 30 days, it is permanently deleted. Therefore, convert or back it up first.
OneDrive without a license	From day 60 without a license, read-only; from day 93, archived and no longer accessible to users and administrators until a license is assigned again or paid billing is activated. After 365 unpaid days, the data can be deleted. Therefore, take over the content before removing the license.
Delete account	The account is recoverable for 30 days, then it is permanently deleted. By default, the manager gets access to the OneDrive, which is retained for 30 days by default (configurable in the SharePoint admin center) and then stays in the recycle bin for 93 days.
Retention	Retention policies and retention labels take precedence over the default process; an eDiscovery hold prevents the OneDrive from being deleted. For unlicensed OneDrives without activated billing, this only applies until possible deletion after 365 unpaid days.

- ☐ Mailbox converted to a shared mailbox, with forwarding if needed, before the license is removed.
- ☐ The person's meetings canceled so that attendees can remove them and booked rooms and equipment become available again.
- ☐ OneDrive content reviewed and taken over by the responsible person.

- ☐ License removed or assigned to another person.
- ☐ Permissions on shared resources removed: groups, Teams, SharePoint sites, permissions on other people's mailboxes (ORP.4.A2).
- ☐ Account deleted as soon as it is no longer needed for the mailbox or forwarding; delete synchronized accounts in on-premises Active Directory, not in Microsoft 365.
- ☐ Documentation of IDs and permission profiles updated (ORP.4.A3).

06

Special Case: Departure with Immediate Effect

For short-notice separations or suspected misuse, block first, then hand over.

If employment ends at short notice or misuse of credentials is a concern, we recommend blocking access at the same time as the conversation and organizing the handover afterward. Microsoft explicitly names termination of employment as a reason to revoke all access and recommends blocking sign-in if an account is suspected of being compromised.

- ☐ Disable the account in Microsoft Entra ID and revoke sessions; if synchronized, also disable it in on-premises Active Directory and reset the password twice.
- ☐ Disable the person's devices registered in Entra ID.
- ☐ Block remote access such as VPN and applications with their own sign-in individually.
- ☐ Wipe and block mobile devices with company data.
- ☐ Change the credentials of shared accounts.

Microsoft Graph PowerShell, according to Microsoft Learn

```
Connect-MgGraph -Scopes "User.ReadWrite.All","Directory.AccessAsUser.All"
$User = Get-MgUser -Search UserPrincipalName:'name@firma.at' -ConsistencyLevel eventual
Update-MgUser -UserId $User.Id -AccountEnabled:$false
Revoke-MgUserSignInSession -UserId $User.Id
Get-MgUserRegisteredDevice -UserId $User.Id -All | ForEach-Object {
    Update-MgDevice -DeviceId $_.Id -AccountEnabled:$false
}
```

07 —

Who Does What

Tasks of HR, supervisors, IT operations, and facility management during a departure.

Responsibilities (roles according to ORP.2.A2 and ORP.4, division as a recommendation)

ROLE	TASKS
HR department	Report the departure date to all affected units, accompany the departure as the designated contact person, and point out confidentiality obligations.
Supervisors	Brief successors and deputies, request handover documentation, and clarify who takes over the mailbox and OneDrive content.
IT operations	Block and delete accounts, remove permissions, take back and wipe devices, and update the documentation of IDs.
Facilities and reception	Collect keys, ID badges, and access authorizations and block them in the access control system.

For each departure, record who completed which item and when. This lets you prove later that access was revoked in time.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

08 —

Sources

All statements are supported by sources. Legislation applies in its current version.

- BSI IT-Grundschutz Compendium, module ORP.2 Personnel (2023 edition)**
ORP.2.A2 Regulated procedure when employees leave, ORP.2.A3 Deputy arrangements, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- BSI IT-Grundschutz Compendium, module ORP.4 Identity and Access Management (2023 edition)**
ORP.4.A2 Revoking permissions, ORP.4.A3 Documentation of IDs and permission profiles
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- Microsoft Learn: Remove a former employee and secure data (overview)**
Steps 1 to 7, retention of the mailbox and OneDrive after license removal and deletion
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- Microsoft Learn: Step 1, Prevent sign-in and block access to Microsoft 365**
Reset the password, sign out of all sessions, block takes up to 24 hours
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...

- 5 **Microsoft Learn: Step 3, Wipe and block a former employee's mobile device**
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- 7 **Microsoft Learn: Revoke user access in Microsoft Entra ID**
Token lifetime, session tokens, reset Active Directory twice, disable devices, wipe only online
learn.microsoft.com/de-de/entra/identity/users/users-revoke-acc...
- 9 **Microsoft Learn: Manage unlicensed OneDrive user accounts**
Read-only from day 60, archive from day 93, deletion risk after 365 unpaid days
learn.microsoft.com/de-de/sharepoint/unlicensed-onedrive-accoun...
- 11 **Microsoft Learn: Restore or remove a recently deleted user**
Recoverable for 30 days
learn.microsoft.com/de-de/entra/fundamentals/users-restore
- 6 **Microsoft Learn: Step 4, Forward email or convert to a shared mailbox**
50 GB limit, account remains in place, cancel meetings
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- 8 **Microsoft Learn: OneDrive retention and deletion**
Manager access, 30-day retention, 93-day recycle bin, archive from day 93 without a license
learn.microsoft.com/de-de/sharepoint/retention-and-deletion
- 10 **Microsoft Learn: No soft-deleted mailbox after removing the license**
Mailbox is disconnected immediately and deleted after 30 days
learn.microsoft.com/de-de/troubleshoot/exchange/user-and-shared...