

CHECKLISTE · TOMORIS TOOLBOX

IT-Offboarding: Checkliste für den Austritt von Mitarbeitenden

Konten, Geräte, Daten und Rechte geordnet beenden, nach BSI IT-Grundschutz und mit den Schritten für Microsoft 365

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/it-offboarding-checkliste

AUF EINEN BLICK

1 h

gilt ein Zugriffstoken von Microsoft Entra ID standardmäßig

30 Tage

bleibt ein gelöscht Konto wiederherstellbar

50 GB

freigegebenes Postfach ohne eigene Lizenz

FÜR WEN

- HR und Personalverantwortliche, die Austritte begleiten
- IT-Leitung und Administration von Microsoft 365 und Microsoft Entra ID
- Führungskräfte, die Übergabe, Nachfolge und Vertretung organisieren

WORUM ES GEHT

Wenn Mitarbeitende das Unternehmen verlassen, bleiben oft Konten, Freigaben und Geräte zurück, die niemand mehr im Blick hat. Diese Checkliste ordnet den Austritt in drei Phasen: vor dem letzten Arbeitstag, am letzten Tag und danach. Sie stützt sich auf die Anforderungen ORP.2.A2 und ORP.4.A2 des IT-Grundschutz-Kompendiums des BSI und nennt für Microsoft 365 die Schritte und Fristen aus der Dokumentation von Microsoft, damit kein Zugang offen bleibt und keine Daten verloren gehen.

Diese Checkliste ist eine Empfehlung von TOMORIS und ersetzt keine arbeits- oder datenschutzrechtliche Beratung. Bezeichnungen, Schritte und Fristen in Microsoft 365 können sich ändern; maßgeblich ist die aktuelle Dokumentation von Microsoft.

INHALT

01	Was beim Austritt geregelt sein muss	2
02	Der Ablauf auf einen Blick	3
03	Vor dem letzten Arbeitstag	3
04	Am letzten Arbeitstag: Zugänge beenden	4
05	Nach dem Austritt: Postfach, OneDrive und Lizenz	5
06	Sonderfall: Austritt mit sofortiger Wirkung	6
07	Wer macht was	7
08	Quellen	8

01

Was beim Austritt geregelt sein muss

Die Anforderungen des BSI IT-Grundschutz-Kompendiums an den Weggang von Mitarbeitenden und an Berechtigungen.

Das IT-Grundschutz-Kompendium des BSI (Edition 2023) regelt den Austritt in der Basis-Anforderung ORP.2.A2 „Geregelte Verfahrensweise beim Weggang von Mitarbeitenden“. Zuständig sind Vorgesetzte und IT-Betrieb. Verlangt wird unter anderem:

- Nachfolgende werden rechtzeitig eingewiesen. Ist eine direkte Übergabe nicht möglich, dokumentieren die Ausscheidenden ihre Aufgaben ausführlich.
- Alle im Rahmen der Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen werden eingezogen.
- Vor der Verabschiedung wird noch einmal auf die Verschwiegenheitsverpflichtungen hingewiesen.
- Notfall- und andere Ablaufpläne werden aktualisiert, alle betroffenen Stellen wie IT-Abteilung oder Sicherheitspersonal informiert.

- Für die anfallenden Aufgaben soll es eine Checkliste geben, und eine feste Ansprechperson der Personalabteilung soll den Weggang begleiten.

Für Konten und Rechte gilt ORP.4.A2: Bei personellen Veränderungen müssen nicht mehr benötigte Benutzendenkennungen und Berechtigungen entfernt werden. Nach ORP.4.A3 ist dokumentiert, welche Kennungen, Gruppen und Rechteprofile bestehen. Diese Dokumentation ist die Grundlage, um beim Austritt nichts zu übersehen.

Reihenfolge und Phasen in diesem Dokument sind eine Empfehlung von TOMORIS. Verbindlich sind Ihre eigenen Regelungen und Verträge; Fristen in Microsoft 365 stammen aus der Dokumentation von Microsoft (Stand siehe Quellen).

02

Der Ablauf auf einen Blick

Drei Phasen vom Bekanntwerden des Austritts bis zur Löschung des Kontos.

Austritt in Phasen (Aufteilung als Empfehlung, Fristen nach Microsoft Learn)



Vorher

Übergabe planen

Aufgaben, Daten, Konten und Geräte erfassen, Nachfolge und Vertretung einweisen, Lösung für Postfach und OneDrive festlegen.



Letzter Tag

Zugänge beenden

Kennwort zurücksetzen, Anmeldung sperren, Sitzungen widerrufen, Geräte, Schlüssel und Ausweise einziehen.



Danach

Daten übergeben

Postfach umwandeln oder weiterleiten, OneDrive-Inhalte übernehmen, Lizenz entziehen, Berechtigungen auf gemeinsame Ressourcen entfernen.



Abschluss

Konto löschen

Das Konto löschen, sobald es nicht mehr für ein freigegebenes Postfach oder eine Weiterleitung gebraucht wird. Es bleibt danach 30 Tage wiederherstellbar.

03

Vor dem letzten Arbeitstag

Übergabe, Vertretung und eine vollständige Liste aller Zugänge, bevor der Zeitdruck beginnt.

- ☐ Nachfolge oder Vertretung ist benannt und eingewiesen; wo keine direkte Übergabe möglich ist, liegt eine Dokumentation der Aufgaben vor (ORP.2.A2, ORP.2.A3).
- ☐ Alle Konten der Person sind erfasst: Microsoft 365 und Entra ID, lokale Anmeldung, Fachanwendungen, VPN, Cloud-Dienste und Portale von Lieferanten (Grundlage ist die Dokumentation nach ORP.4.A3).
- ☐ Erhöhte Rechte sind bekannt: Administrationsrollen, Berechtigungen auf fremde Postfächer, Besitz von Teams, Gruppen und SharePoint-Websites.

- ☐ Gemeinsam genutzte Zugangsdaten, die die Person kennt, sind aufgelistet, damit sie nach dem Austritt geändert werden.
- ☐ Dienstliche Daten liegen in der vorgesehenen gemeinsamen Ablage und nicht nur lokal oder im persönlichen OneDrive.
- ☐ Für das Postfach ist entschieden: Umwandlung in ein freigegebenes Postfach oder Weiterleitung an eine Kollegin oder einen Kollegen.
- ☐ Für den OneDrive ist festgelegt, wer die Inhalte übernimmt. In Microsoft Entra ID ist die vorgesetzte Person eingetragen; sie erhält beim Löschen des Kontos standardmäßig Zugriff.
- ☐ Ausgegebene Geräte, Sicherheitsschlüssel, Schlüssel, Ausweise und Zutrittsmittel stehen in einer Liste zum Abhaken.
- ☐ Notfallpläne, Kontaktlisten und Bereitschaftspläne sind aktualisiert (ORP.2.A2).
- ☐ Betroffene Stellen wie IT, Empfang, Gebäudeverwaltung und externe Dienstleister kennen den Austrittstermin (ORP.2.A2).

04 —

Am letzten Arbeitstag: Zugänge beenden

Kennwort zurücksetzen, Anmeldung sperren, Sitzungen widerrufen, Geräte und Zutrittsmittel einziehen.

1

Kennwort zurücksetzen und abmelden

Im Microsoft 365 Admin Center das Kennwort zurücksetzen und die Person von allen Sitzungen abmelden. Laut Microsoft verhindert das Zurücksetzen die Anmeldung sofort, eine Anmeldesperre kann dagegen bis zu 24 Stunden brauchen. Ein Zugriffstoken gilt bis zu einer Stunde weiter.

2

Anmeldung sperren und Sitzungen widerrufen

Die Anmeldung blockieren, im Microsoft Entra Admin Center also „Konto aktiviert“ deaktivieren und danach „Sitzungen widerrufen“ wählen. Damit erhält die Person für keine an Entra ID angebundene Anwendung mehr neue Token.

3

Lokales Active Directory nicht vergessen

Werden Konten aus einem lokalen Active Directory synchronisiert, das Konto auch dort deaktivieren und das Kennwort zurücksetzen. Microsoft empfiehlt, es zweimal zurückzusetzen, um das Risiko von Pass-the-Hash zu mindern; ist das Konto sicher nicht kompromittiert, genügt einmal.

4

Mobile Geräte löschen und blockieren

Für dienstlich genutzte Smartphones im Exchange Admin Center die Firmendaten aus der Ferne löschen und den Zugriff blockieren, bei Verwaltung mit Intune über Intune. Eine Löschung greift nur, wenn das Gerät online ist; offline bleiben lokal gespeicherte Daten erreichbar.

5

Geräte, Schlüssel und Ausweise einziehen

Notebook, Smartphone, Sicherheitsschlüssel, Schlüssel, Ausweise und Zutrittsberechtigungen zurücknehmen und in der Liste abhaken (ORP.2.A2). Zutrittsberechtigungen im Schließ- oder Zutrittssystem sperren.

6

Anwendungen außerhalb von Entra ID

Anwendungen mit eigener Anmeldung oder eigenen Sitzungen einzeln sperren. Microsoft weist darauf hin, dass Entra ID von Anwendungen ausgestellte Sitzungstoken nicht widerrufen kann; die automatische Aufhebung der Bereitstellung schließt diese Lücke, wo die Anwendung sie unterstützt.

7

Gemeinsame Zugangsdaten ändern

Kennwörter gemeinsam genutzter Konten und Zugänge ändern, die die Person kannte. Die Liste aus der Vorbereitung dient als Vorlage.

Vor der Verabschiedung noch einmal auf bestehende Verschwiegenheitsverpflichtungen hinweisen (ORP.2.A2).

05

Nach dem Austritt: Postfach, OneDrive und Lizenz

Was Microsoft 365 mit Postfach, OneDrive und Konto macht und welche Fristen dabei laufen.

Verhalten und Fristen in Microsoft 365 (laut Microsoft Learn, gelesen am 25.10.2026)

THEMA	WAS GILT
Freigegebenes Postfach	Die Umwandlung erhält alle E-Mails und den Kalender. Ohne Lizenz bis 50 GB, darüber braucht das Postfach eine Lizenz. Das Konto darf dafür nicht gelöscht werden.
Weiterleitung	Leitet nur neue E-Mails an die Nachfolge weiter. Konto und Postfach müssen bestehen bleiben; ohne Lizenz geht das nur über ein freigegebenes Postfach mit Weiterleitung.
Lizenz entziehen	Ein normales Benutzerpostfach wird sofort getrennt und ist nicht mehr zugänglich; nach 30 Tagen wird es endgültig gelöscht. Deshalb vorher umwandeln oder sichern.
OneDrive ohne Lizenz	Ab dem 60. Tag ohne Lizenz nur noch lesbar, ab dem 93. Tag archiviert und für Nutzer und Administration nicht mehr zugänglich, bis wieder eine Lizenz zugewiesen oder die kostenpflichtige Abrechnung aktiviert wird. Nach 365 unbezahlten Tagen können die Daten gelöscht werden. Inhalte deshalb vor dem Lizenzentzug übernehmen.
Konto löschen	Das Konto ist 30 Tage wiederherstellbar, danach wird es endgültig gelöscht. Die vorgesetzte Person erhält standardmäßig Zugriff auf den OneDrive, der standardmäßig 30 Tage aufbewahrt wird (einstellbar im SharePoint Admin Center) und danach 93 Tage im Papierkorb liegt.

Aufbewahrung

Aufbewahrungsrichtlinien und -bezeichnungen gehen dem Standardablauf vor; ein eDiscovery-Hold verhindert das Löschen des OneDrive. Bei nicht lizenzierten OneDrives ohne aktivierte Abrechnung gilt das nur bis zur möglichen Löschung nach 365 unbezahlten Tagen.

- ☐ Postfach in ein freigegebenes Postfach umgewandelt, bei Bedarf mit Weiterleitung, bevor die Lizenz entzogen wird.
- ☐ Besprechungen der Person abgesagt, damit Teilnehmende sie entfernen können und gebuchte Räume und Geräte wieder frei sind.
- ☐ OneDrive-Inhalte von der zuständigen Person gesichtet und übernommen.
- ☐ Lizenz entzogen oder einer anderen Person zugewiesen.
- ☐ Berechtigungen auf gemeinsame Ressourcen entfernt: Gruppen, Teams, SharePoint-Websites, Berechtigungen auf fremde Postfächer (ORP.4.A2).
- ☐ Konto gelöscht, sobald es nicht mehr für Postfach oder Weiterleitung gebraucht wird; synchronisierte Konten im lokalen Active Directory löschen, nicht in Microsoft 365.
- ☐ Dokumentation der Kennungen und Rechteprofile aktualisiert (ORP.4.A3).

06

Sonderfall: Austritt mit sofortiger Wirkung

Bei kurzfristiger Trennung oder befürchtetem Missbrauch zuerst sperren, dann übergeben.

Endet das Arbeitsverhältnis kurzfristig oder ist ein Missbrauch der Zugangsdaten zu befürchten, empfehlen wir, die Zugänge zeitgleich mit dem Gespräch zu sperren und die Übergabe danach zu organisieren. Microsoft nennt die Beendigung eines Arbeitsverhältnisses ausdrücklich als Anlass, alle Zugriffe zu widerrufen, und empfiehlt bei Verdacht auf ein kompromittiertes Konto, die Anmeldung zu blockieren.

- ☐ Konto in Microsoft Entra ID deaktivieren und Sitzungen widerrufen; bei Synchronisation zusätzlich im lokalen Active Directory deaktivieren und das Kennwort zweimal zurücksetzen.
- ☐ In Entra ID registrierte Geräte der Person deaktivieren.
- ☐ Fernzugänge wie VPN sowie Anwendungen mit eigener Anmeldung einzeln sperren.
- ☐ Mobile Geräte mit Firmendaten löschen und blockieren.
- ☐ Zugangsdaten gemeinsam genutzter Konten ändern.

Microsoft Graph PowerShell, nach 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

Wer macht was

Aufgaben von Personalabteilung, Vorgesetzten, IT-Betrieb und Gebäudeverwaltung beim Austritt.

Zuständigkeiten (Rollen nach ORP.2.A2 und ORP.4, Aufteilung als Empfehlung)

ROLLE	AUFGABEN
Personalabteilung	Austrittstermin an alle betroffenen Stellen melden, den Austritt als feste Ansprechperson begleiten, auf Verschwiegenheitsverpflichtungen hinweisen.
Vorgesetzte	Nachfolge und Vertretung einweisen, Übergabedokumentation einfordern, Übernahme von Postfach und OneDrive-Inhalten klären.
IT-Betrieb	Konten sperren und löschen, Berechtigungen entfernen, Geräte zurücknehmen und löschen, Dokumentation der Kennungen aktualisieren.
Gebäude und Empfang	Schlüssel, Ausweise und Zutrittsberechtigungen einziehen und im Zutrittssystem sperren.

Halten Sie für jeden Austritt fest, wer welchen Punkt wann erledigt hat. So lässt sich später nachweisen, dass Zugänge rechtzeitig entzogen wurden.

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **BSI IT-Grundschutz-Kompendium, Baustein ORP.2 Personal (Edition 2023)**
ORP.2.A2 Geregelte Verfahrensweise beim Weggang von Mitarbeitenden, ORP.2.A3 Vertretungsregelungen, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 2 **BSI IT-Grundschutz-Kompendium, Baustein ORP.4 Identitäts- und Berechtigungsmanagement (Edition 2023)**
ORP.4.A2 Entzug von Berechtigungen, ORP.4.A3 Dokumentation der Kennungen und Rechteprofile
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **Microsoft Learn: Entfernen ehemaliger Mitarbeitender und Schützen von Daten (Übersicht)**
Schritte 1 bis 7, Aufbewahrung von Postfach und OneDrive nach Lizenzentzug und Löschung
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- 4 **Microsoft Learn: Schritt 1, Anmeldung verhindern und Zugriff auf Microsoft 365 blockieren**
Kennwort zurücksetzen, von allen Sitzungen abmelden, Sperre bis zu 24 Stunden
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- 5 **Microsoft Learn: Schritt 3, Mobilgerät ehemaliger Mitarbeitender löschen und blockieren**
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- 6 **Microsoft Learn: Schritt 4, E-Mails weiterleiten oder in ein freigegebenes Postfach umwandeln**
50-GB-Grenze, Konto bleibt bestehen, Besprechungen absagen
learn.microsoft.com/de-de/microsoft-365/admin/add-users/remove-...
- 7 **Microsoft Learn: Widerrufen des Benutzerzugriffs in Microsoft Entra ID**
Token-Laufzeit, Sitzungstoken, Active Directory zweimal zurücksetzen, Geräte deaktivieren, Löschen nur online
learn.microsoft.com/de-de/entra/identity/users/users-revoke-acc...
- 8 **Microsoft Learn: OneDrive-Aufbewahrung und -Löschung**
Zugriff der vorgesetzten Person, 30 Tage Aufbewahrung, 93 Tage Papierkorb, Archiv ab dem 93. Tag ohne Lizenz
learn.microsoft.com/de-de/sharepoint/retention-and-deletion
- 9 **Microsoft Learn: Nicht lizenzierte OneDrive-Benutzerkonten verwalten**
Schreibschutz ab Tag 60, Archiv ab Tag 93, Löschrisko nach 365 unbezahlten Tagen
learn.microsoft.com/de-de/sharepoint/unlicensed-onedrive-accoun...
- 10 **Microsoft Learn: Kein vorläufig gelöscht Postfach nach Entfernen der Lizenz**
Postfach wird sofort getrennt und nach 30 Tagen gelöscht
learn.microsoft.com/de-de/troubleshoot/exchange/user-and-shared...
- 11 **Microsoft Learn: Wiederherstellen oder Entfernen eines kürzlich gelöschten Benutzers**
30 Tage wiederherstellbar
learn.microsoft.com/de-de/entra/fundamentals/users-restore