

CHECKLIST · TOMORIS TOOLBOX

IT Onboarding: Checklist for New Employees Joining

Set up account, permissions, device, first sign-in, data secrecy and training in an orderly way, based on BSI IT-Grundschutz and the DSGVO, with the steps for Microsoft 365

UPDATED

Oct 25, 2026

LENGTH

PDF, 7 pages

ONLINE

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

AT A GLANCE

ORP.2

BSI: structured onboarding of new employees

§ 6

DSG: commit employees to data secrecy

1 h

default validity of a Temporary Access Pass

30 days

maximum configurable validity of the access pass

WHO IT IS FOR

- HR and people managers who prepare new hires
- IT management and administrators of Microsoft 365 and Microsoft Entra ID
- Managers who define tasks, permissions and onboarding

WHAT THIS COVERS

Onboarding decides whether accounts are set up cleanly, permissions are limited to what is needed and new colleagues work securely from the start. This checklist organizes onboarding into three phases: before the first working day, on the first day and in the first weeks. It is based on the modules ORP.2, ORP.3 and ORP.4 of the BSI IT-Grundschutz Compendium (IT baseline protection of the German Federal Office for Information Security) and on data secrecy under § 6 DSG (Austrian Data Protection Act). For Microsoft 365, it lists the steps from creating the user through the Temporary Access Pass to automation. It is the counterpart to the IT offboarding checklist.

This checklist is a TOMORIS recommendation and does not replace advice on employment or data protection law. Adapt it to your business. Names, default values and licenses in Microsoft 365 can change; Microsoft's current documentation and the DSG and GDPR as currently in force are authoritative.

CONTENTS

01	What must be settled when someone joins	2
02	The process at a glance	3
03	Before the first working day	3
04	On the first working day	4
05	In the first weeks	5
06	Steps in Microsoft 365	5
07	Role changes and external staff	6
08	Who does what	6
09	Sources	7

01 —

What must be settled when someone joins

Onboarding, permissions as needed, commitment and training

HR and supervisors must ensure that new employees are onboarded and informed about rules, instructions and procedures. A checklist and a fixed contact person should help (BSI ORP.2.A1). User IDs and permissions may only be granted based on actual need (ORP.4.A2). Four areas therefore belong to every onboarding:

- Account and permissions: clearly assigned to one person, only what the task requires, documented (ORP.4.A1 to A3).
- Devices and access: issue physical and logical access means and document the issue (ORP.4.A5 to A7); record device handover as well (TOMORIS recommendation).

- Commitment: data secrecy under § 6 DSG, compliance with laws and internal rules (ORP.2.A14), processing of personal data only on instruction (Art. 29 and 32(4) GDPR).
- Briefing and training: secure use of IT and task-based training (ORP.3.A3, A6).

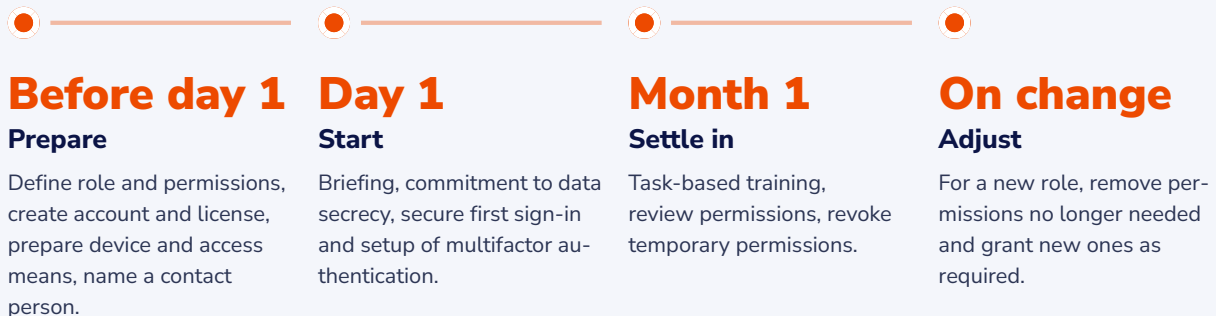
This checklist is a TOMORIS recommendation. BSI IT-Grundschutz is not a legal requirement in Austria but a standard the checklist follows; § 6 DSG and the GDPR apply directly. Leaving the company is covered by the IT offboarding checklist.

02

The process at a glance

Three phases until onboarding is complete, plus the case of a role change

Phases of IT onboarding (TOMORIS recommendation)



03

Before the first working day

Prepare account, permissions, device and contact person

- ☐ HR reports the new hire, function and start date to IT and supervisors in good time.
- ☐ Required permissions derived from the function; permissions beyond the standard only with additional justification and review (ORP.4.A2).
- ☐ Account created and clearly assigned to one person; created only through a separate administrative role (ORP.4.A1, A2).
- ☐ Account, groups and permission profile documented (ORP.4.A3).
- ☐ Physical and logical access defined; issue of keys, smart cards or tokens is documented (ORP.4.A5 to A7).

- ☐ Device prepared and added to inventory; license assigned in Microsoft 365.
- ☐ Qualifications required for the position clarified (ORP.2.A15); if needed, trustworthiness details checked, such as the résumé (ORP.2.A7).
- ☐ Contact person or buddy for onboarding named (ORP.2.A1).
- ☐ For external staff: written confidentiality agreement before access to confidential information is granted (ORP.2.A5).

04 —

On the first working day

Brief, commit, sign in securely

1

Brief

Inform about applicable rules, instructions and procedures (ORP.2.A1); brief on the secure use of IT components and provide binding, understandable policies (ORP.3.A3).

2

Commit and instruct

Unless already bound by law, contractually oblige the person to transmit personal data only on instruction and to maintain data secrecy even after the employment ends; instruct them on transmission orders and the consequences of a breach (§ 6 paras. 2 and 3 DSG). Commit them to compliance with laws and internal rules (ORP.2.A14).

3

Sign in securely for the first time

For the first sign-in, issue a Temporary Access Pass that the person uses to set up their own sign-in methods. TOMORIS recommends not sending passwords by email and handing over the access pass in person or through a separate channel.

4

Set up multifactor sign-in

Have the person register an authenticator app or passkey. The MFA in Microsoft 365 checklist covers rollout and methods in detail.

5

Hand over device and access means

Hand over keys, smart cards and tokens and document the issue (ORP.4.A5 to A7), and the device as well (TOMORIS recommendation). Instruct the person to keep passwords secret (ORP.4.A8).

6

Explain the reporting path

Show how to report suspicious emails and security incidents and who the contact person is (TOMORIS recommendation).

05 —

In the first weeks

Train, review permissions, complete onboarding

- ☐ Trained on information security according to tasks and responsibilities (ORP.3.A6).
- ☐ Informed that information from work is for internal use only and that information security also applies outside working hours (ORP.2.A14).
- ☐ Tasks and responsibilities documented (ORP.2.A14).
- ☐ Permissions matched against actual tasks; documentation and granted permissions are consistent (ORP.4.A3).
- ☐ Temporarily granted permissions, for example for onboarding, revoked (derived from ORP.4.A2).
- ☐ Deputy arrangements for the new person's tasks in place (ORP.2.A3).
- ☐ Onboarding completed with supervisor and contact person, and feedback on the checklist collected (TOMORIS recommendation).

06 —

Steps in Microsoft 365

Users, Temporary Access Pass, devices and automation

Create users	Create users and assign licenses in the Microsoft 365 admin center. Microsoft recommends roles with the least privileges; Global Administrator should be limited to emergency scenarios.
Temporary Access Pass (TAP)	Time-limited passcode for one or more sign-ins, which users use to set up passwordless methods. Enable it first in the authentication methods policy and select users or groups. Valid for 1 to 8 hours out of the box, 1 hour by default; configurable in the policy from 10 minutes to 30 days; one-time use can be enforced.
Windows Autopilot	Sets up and preconfigures new Windows devices so they are ready for use; also used for resetting and recovery. Automatic enrollment in Intune requires Entra ID P1 or P2.
Lifecycle workflows	Automate tasks for joiners, movers and leavers, such as an email to the manager seven days before the start date or creating temporary passwords. Require licenses for Microsoft Entra ID Governance or Microsoft Entra Suite.

Names, default values and license terms in Microsoft 365 can change; Microsoft's current documentation is authoritative. Password rules are best set in a dedicated password policy.

07

Role changes and external staff

When tasks change or external people join the work

- ☐ When staff changes occur, remove IDs and permissions no longer needed (ORP.4.A2) instead of only adding new permissions.
- ☐ Commit external staff to laws, regulations and internal rules just like your own employees (ORP.2.A4).
- ☐ Supervise short-term external staff in security-relevant areas, and brief long-term external staff like your own employees (ORP.2.A4).
- ☐ Create accounts for external staff with an expiration date and revoke access rights when the engagement ends (ORP.2.A4; expiration date as a TOMORIS recommendation).

08

Who does what

Responsibilities in onboarding

Responsibilities (split based on BSI ORP.2 and ORP.4)

ROLE	ONBOARDING TASK
HR	Reports the new hire, ensures onboarding together with supervisors, obtains the commitment to data secrecy.
Supervisors	Define tasks, required permissions and deputies, name the contact person, approve special permissions.
IT operations	Creates account, groups and permissions, documents them, prepares device and access means, issues the access pass.
Data protection	Provides the text and instruction on data secrecy.
New employees	Set up their sign-in methods, keep passwords secret, attend briefing and training.

The exact split is a recommendation; what matters is that every task has a responsible person. Complete the checklist for each new hire and file it in the personnel file or the IT documentation.

NEXT STEP

Check It Yourself or Put It into Practice Together

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

09 —

Sources

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

- 1 **BSI IT-Grundschutz Compendium, module ORP.2 Personnel (Edition 2023)**
ORP.2.A1, A3, A4, A5, A7, A14, A15, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 2 **BSI IT-Grundschutz Compendium, module ORP.3 Security Awareness and Training (Edition 2023)**
ORP.3.A3, A6, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 3 **BSI IT-Grundschutz Compendium, module ORP.4 Identity and Access Management (Edition 2023)**
ORP.4.A1 to A3, A5 to A8, accessed October 25, 2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 4 **Datenschutzgesetz (DSG, Austrian Data Protection Act), version in force in the RIS**
§ 6 data secrecy, accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 5 **Regulation (EU) 2016/679 (GDPR), German version on EUR-Lex**
Art. 29 and Art. 32(4), accessed October 25, 2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 6 **Microsoft Learn: Configure Temporary Access Pass in Microsoft Entra ID**
Purpose, policy, lifetime, one-time use, accessed October 25, 2026
learn.microsoft.com/de-de/entra/identity/authentication/howto-a...
- 7 **Microsoft Learn: Add users and assign licenses**
Least-privileged roles, license assignment, accessed October 25, 2026
learn.microsoft.com/de-de/microsoft-365/admin/add-users/add-use...
- 8 **Microsoft Learn: Windows Autopilot overview**
Purpose; Entra ID P1 or P2 for Intune enrollment, accessed October 25, 2026
learn.microsoft.com/de-de/autopilot/overview
- 9 **Microsoft Learn: What are lifecycle workflows?**
Phases, example, license requirements, accessed October 25, 2026
learn.microsoft.com/de-de/entra/id-governance/what-are-lifecycl...