

CHECKLIST · TOMORIS TOOLBOX

Teams and SharePoint: Checklist for Secure Sharing

Settings with their location in the admin center, checklists for the organization and each team, monitoring with reports and reviews, based on Microsoft Learn

UPDATED

Oct 25, 2026

LENGTH

PDF, 11 pages

ONLINE

tomoris.com/en/downloads/teams-sharepoint-freigaben-checkliste

AT A GLANCE

4 levels

Sharing from "Anyone" to "Only people in your organization"

1 hour

usually, until guests lose access after a restriction

28 days

Period covered by over-sharing activity reports

Oct 2026

SharePoint OTP ends; guests need an Entra B2B account

WHO IT IS FOR

- Administrators of Microsoft 365, SharePoint, and Teams in small and medium-sized businesses
- Data protection and information security teams who assess and monitor sharing with external parties
- IT managers who set rules for collaboration with customers, partners, and suppliers

WHAT THIS COVERS

In Microsoft 365, collaboration with external parties depends on settings in SharePoint, Microsoft Entra ID, Microsoft 365, and Teams. This checklist organizes them for administrators and data protection teams. It covers the terms guest access, external access, and sharing link, recommended baseline settings with their location in the admin center, and one checklist each for the organization and for every team. It also covers sensitivity labels, ongoing monitoring with reports and access reviews, and team owners and lifecycle. In addition, it includes the changes from 2025 and 2026 and the license requirement for each feature according to Microsoft Learn.

This checklist is a TOMORIS recommendation and must be adapted to your own environment; it does not replace legal advice. Microsoft continually changes features, names, menus, defaults, and licenses: the linked Microsoft Learn pages in their current version are authoritative, and for obligations, the legal text of the GDPR and NISG 2026 in its current version.

CONTENTS

01	What It's About: Guests, External Access, Sharing Links	2
02	What Changed in 2025 and 2026	4
03	Baseline Settings for SharePoint and OneDrive	4
04	Baseline Settings in Entra ID and Teams	5
05	Checklists for the Organization and for Each Team	6
06	Sensitivity Labels for Teams, Groups, and Sites	8
07	Ongoing Monitoring: Reports and Reviews	9
08	Team Owners and Lifecycle	9
09	Sources	10

01 —

What It's About: Guests, External Access, Sharing Links

Four ways external parties get to content, the types of sharing links, and what is required by law.

External parties reach content in Microsoft 365 as a guest with their own account, via a sharing link, or in a shared Teams channel; via external access in Teams, they only chat, call, and meet. According to Microsoft, a new team also creates a Microsoft 365 group and a SharePoint team site, to which the guest sharing settings of groups and Teams apply. If Entra ID is more restrictive than SharePoint or OneDrive, Entra ID prevails.

Guest access (Microsoft Entra B2B)	A guest account in your Entra ID for teams, channels, chats, meetings, and files, including with Conditional Access and MFA. Since 2026, SharePoint and OneDrive in commercial tenants always create a guest account when files, folders, and sites are shared with specific external people, but not for "Anyone" links.
External access (federation)	Chat, calls, and meetings with people from other Microsoft 365 organizations, without a guest account and without access to your teams, sites, or other resources.
Shared channel (B2B direct connect)	People from another Entra tenant work in a channel of your team with their own account, without a guest account; B2B direct connect is blocked by default and requires both organizations to enable it.
"Anyone" link	Opens without sign-in and can be forwarded; according to Microsoft, access cannot be audited. Deleting it revokes it for everyone.
"People in your organization" link	Only for signed-in members of your directory, not for guests; if forwarded, it works for everyone in the organization.
"Specific people" link	Only for the people named, internal and external, after signing in as that person; the file also appears for them in search and Copilot.

What is required and what is recommended

REQUIREMENT	FOR WHOM	BASIS
appropriate measures for the confidentiality of systems and services, with regard to unauthorized disclosure, and their regular review	Controllers and processors	Art. 32(1)(b) and (d) and (2) GDPR
access control policies; restrict third-party rights by scope and duration, review them as planned, and document them	essential and important entities (§§ 24 to 26 NISG 2026, Austrian Network and Information Systems Security Act 2026); NISG since Oct 1, 2026, NISV (Austrian NIS Regulation) since the end of that day	§ 32 para. 4 lit. i NISG 2026; § 2 NISV 2026 with Annex points 11.2.2(d) and 11.2.3 IR (EU) 2024/2690
all items in this checklist; the GDPR and NISG 2026 do not prescribe specific settings	all tenants	TOMORIS recommendation based on Microsoft Learn

02 —

What Changed in 2025 and 2026

Entra B2B becomes mandatory for SharePoint, the SharePoint one-time passcode ends, guests sign in differently.

- For the end of the SharePoint one-time passcode (the Entra B2B email one-time passcode remains), Microsoft advises: create a guest account with the same email address as for the old link, or share the item again; there are no exceptions. Check domain lists that exist only in SharePoint and transfer them to Entra ID if necessary.
- Microsoft Learn describes (as of October 2026) expiration policies for “People in your organization” links as well; existing links are checked against their creation date when opened.
- With a Copilot license (at least one person), SharePoint administrators receive, according to Microsoft, the Copilot-supporting features of SharePoint Advanced Management; some still require the Plan 1 add-on (Section 07).

Changes according to Microsoft Learn, accessed October 25, 2026



July 2025

New guest sign-in

Guests sign in on their own organization's page and then return; rolled out by the end of 2025.



January 2026

Add-on for guests

New guest reviews with “inactive users” or recommendations based on group membership only with the Entra ID Governance for guests add-on.



May to July 2026

Entra B2B mandatory

Microsoft has enabled Entra B2B for new sharing from SharePoint and OneDrive in commercial tenants; it cannot be turned off.



Oct 2026

SharePoint passcode ends

During October, the SharePoint one-time passcode ends in commercial tenants: external users without a guest account get “Access denied” for old “Specific people” links.

03 —

Baseline Settings for SharePoint and OneDrive

The more restrictive value of organization and site applies; defaults and recommendations.

You set the sharing level in the SharePoint admin center under Policies > Sharing, separately for SharePoint and OneDrive; OneDrive cannot be more permissive. According to Microsoft, external sharing is enabled by default. Per site (Active sites > site > Settings > More sharing settings), you can only make it stricter; the more restrictive value always applies. SharePoint administrators can change this, site owners cannot (exception: a label with a sharing setting, Section 06).

Default per site according to Microsoft: OneDrive and the root site (mandant.sharepoint.com) “Anyone”; group-connected sites, including those of Teams, “New and existing guests” if group owners are allowed to add external users, otherwise only existing guests; all others “Only people in your organization.”

Recommended baseline settings under Policies > Sharing (TOMORIS recommendation; setting names shortened)

SETTING	TOMORIS RECOMMENDATION
External sharing for SharePoint	"New and existing guests"; "Anyone" only if anonymous links are needed. Microsoft also does not recommend "Existing guests," because guests get into the directory in other ways.
External sharing for OneDrive	the same as or stricter than SharePoint; according to Microsoft, file requests in OneDrive require "Anyone" and edit permissions for "Anyone" links
File and folder links (default link type)	"Specific people," or "Only people in your organization" if sharing is mostly internal; never "Anyone with the link"
Default permission for sharing links	"View"; choose edit deliberately on a case-by-case basis
Advanced settings for Anyone links	Expiration required, for example 30 days, and "View" only; according to Microsoft, file requests require edit permissions, or "View and upload" for folders. According to Microsoft, a shorter period also applies to existing links.
Limit external sharing by domain	Allow list for a fixed group of partners (up to 5,000 domains), otherwise a block list; better centrally in Entra ID (Section 04)
Allow only specific security groups to share externally	restrict to one group for high protection needs
Allow guests to share items they don't own	off
Guest access expires after this many days	on, matching the project duration, for example 90 days; can be set differently per site

According to Microsoft, guests usually lose access within one hour after a restriction; if sharing is turned back on, they regain it. According to Microsoft, confidential content belongs on sites without external sharing, and work with external parties belongs on separate sites.

04

Baseline Settings in Entra ID and Teams

Who may invite guests, from which domains, with MFA, and what guests and external contacts may do in Teams.

Recommended baseline settings (TOMORIS recommendation; defaults and locations according to Microsoft Learn)

SETTING	LOCATION	RECOMMENDATION
Guest invite settings (default: everyone, including guests)	Entra ID > External Identities > External collaboration settings	Members and specific administrator roles; guests don't invite guests. Stricter: only administrator roles and the Guest Inviter role.

Guest user access (default: limited)	same location	with guests from several companies, "restricted to properties and memberships of their own directory objects": guests see no other users in the directory; in jointly shared folders, they still see each other
Collaboration restrictions	same location	Block list of unwanted domains or allow list of fixed partner domains; also applies to SharePoint, Teams, and groups
MFA for guests	Entra ID > Conditional Access > Policies	Policy with MFA for guests (Entra ID P1 or P2); trust MFA from partner tenants only selectively
Guest access in Teams	Teams admin center > Users > Guest access	on if guests collaborate in Teams; decide deliberately on calls, screen sharing, and chat for guests
Guest access for Microsoft 365 groups (default: on)	Microsoft 365 admin center > Settings > Org settings > Services > Microsoft 365 Groups	Guest access to group content only if guests collaborate in Teams; whether owners may add external users also determines the default sharing level of team sites
External access (default: all domains)	Teams admin center > Users > External access	"Allow only specific external domains" for a fixed group of partners; unmanaged Teams accounts only if needed, without contact initiated from outside

Your tenant is responsible for guest MFA; you can trust the partner organization's MFA via cross-tenant access settings (trust settings, Entra ID P1). Blocked domains in external access do not block subdomains by default; `Set-CsTenantFederationConfiguration -BlockAllSubdomains $True` changes this.

Licenses according to Microsoft: guest access in Teams is included in Microsoft 365 Business Standard, Enterprise, and Education, with no additional license; the Entra External ID billing model applies to guests. Guests without a license only have basic collaboration, for example in Office on the web.

05

Checklists for the Organization and for Each Team

Configure once in the tenant and document; check for each team and site before the first guest.

For the organization: configure once, document, and review at fixed intervals.

- ☐ Responsibility for changing sharing settings is clarified; there is a written rule on what may be shared with whom and through which channel.
- ☐ Settings from Section 03 implemented: sharing level chosen deliberately, default link "Specific people" with "View," "Anyone" links off or with expiration, guest access expiration on.
- ☐ Settings from Section 04 implemented: guest invitations restricted, domain rules centrally in Entra ID, guest and external access in Teams set appropriately.
- ☐ Conditional Access policy with MFA for guests active and tested beforehand with test accounts.

- ☐ Sensitivity labels for teams, groups, and sites enabled, with at least one label without guests (Section 06).
- ☐ Earlier sharing with the SharePoint one-time passcode reviewed: anyone who still needs access has a guest account with the same email address.
- ☐ Expiration policy for groups, for example 180 days with a fallback address, and policy for ownerless groups set up (Section 08); when an owner leaves, the role is handed over beforehand.
- ☐ Monitoring scheduled (Section 07): monthly activity or sharing reports, quarterly permissions and the "Guest users" page in the Microsoft 365 admin center, guests reviewed and documented at project end and at defined intervals (Annex point 11.2.3 IR), these settings checked annually.
- ☐ Sharing and OneDrive content handed over when someone leaves; guest accounts deleted after a partnership ends.

For each team and site, before the first guest:

- ☐ Purpose and partner companies described; confidential content is in a separate team without external sharing.
- ☐ At least two owners from your own organization; team set to "Private" if not everyone should be able to read along; appropriate sensitivity label applied.
- ☐ Site sharing level: with guests "New and existing guests," internal "Only people in your organization"; default link stricter than the organization's if needed.
- ☐ Sharing limited to the partners' domains (Advanced settings for external sharing > Limit sharing by domain) and guest access expiration adjusted to the project duration.
- ☐ Every guest has a responsible person. After being added to a team, access can take up to 12 hours; guests added directly to the group do not receive an invitation email, so someone from the team informs them.
- ☐ Members know: guests carry the label "(Guest)," and in jointly shared folders they see each other under "Manage access"; only what the guest needs is shared.
- ☐ At project end, guests removed and guest accounts no longer needed deleted; a guest who leaves the team remains in the directory.

06 —

Sensitivity Labels for Teams, Groups, and Sites

Container labels control privacy, guests, and sharing per team; files need their own labels.

Labels from Microsoft Purview in the “Groups & sites” scope define per team: privacy (public or private), external user access (whether owners may add guests), the site's external sharing level, access from unmanaged devices, and authentication contexts (both with Conditional Access). Microsoft also applies the team's label to the group and site.

1

Enable for containers

Set `EnableMIPLabels` in Entra ID to `True` via Microsoft Graph PowerShell, then run `Execute-AzureAdLabelSync` in Security & Compliance PowerShell; it takes up to 24 hours until they are available in Entra ID.

2

Create labels

“Groups & sites” scope. TOMORIS example: “Internal” (private, no guests, sharing within the organization only) and “Partner” (private, guests allowed, “New and existing guests”).

3

Test with a few people

Publish to test accounts; for a new label, wait at least one hour (24 hours with shared channel controls), for a changed label 24 hours; create a team with it, then publish to everyone.

4

Label existing teams

SharePoint admin center > Active sites: show the “Sensitivity” column, apply the label via the Policies tab; for many sites, use PowerShell.

According to Microsoft, files do not inherit the container's label; for that, there are labels for Office files in SharePoint and OneDrive. If the label controls external sharing, site owners can change it by switching the label; invited guests keep their access if “External user access” is turned off later.

Licenses according to Microsoft: at least one active Entra ID P1 license in the tenant; according to the Purview service description, manual labeling is included in Microsoft 365 Business Premium, E3, and E5, among others, automatic labeling only with E5 or Purview add-on licenses; authentication contexts via labels only with Microsoft 365 E5, Information Protection and Governance, or Office 365 E5.

07 —

Ongoing Monitoring: Reports and Reviews

Where oversharing becomes visible, who confirms guests' need for access, and which license Microsoft lists for it.

Monitoring tools (license information according to Microsoft Learn, without prices)

TOOL	WHAT IT SHOWS OR DOES	LICENSE ACCORDING TO MICROSOFT
Site sharing report (Settings > Site usage > Shared with external users)	CSV with files, people, permissions, and links, including to guests; without "Anyone" links	no additional license mentioned; for site administrators
Data access governance (SharePoint admin center > Reports)	Permissions of all sites; sites with many new sharing links or sharing with "Everyone except external users" in 28 days	SharePoint Advanced Management: base subscription plus Copilot license, Plan 1 add-on, or Microsoft 365 E7; with E5 alone, only activity reports for up to 10,000 sites
Access review for guests (Entra ID Governance)	Guests or owners confirm the need for access, also on a recurring basis for all groups with guests; for selected teams, block denied users for 30 days, then delete them	Entra ID P2 or Entra ID Governance; for reviews of inactive guests or with recommendations based on group membership, additionally at least one Entra ID Governance or Entra Suite license and the add-on for guests with an Azure subscription

Microsoft recommends the permissions report quarterly and activity reports monthly; without SharePoint Advanced Management, data collection must first be turned on. Base subscription according to the prerequisites page: Office 365 E3, E5, A5 or Microsoft 365 E1, E3, E5, A5; it does not list Business plans as a base subscription, so check in the admin center beforehand.

Common mistakes (compiled by TOMORIS): "Anyone with the link" as the default; "Anyone" links without expiration; sharing turned off and on again so that guests regain their access; only SharePoint restricted; confidential content and partner work on one site; container label mistaken for file protection; guests never reviewed.

08 —

Team Owners and Lifecycle

According to Microsoft, teams need an owner to manage members; two policies help.

Expiration policy for Microsoft 365 groups

Microsoft Entra admin center > Groups > All groups > Expiration

Lifetime of 30 days or more. Groups in use are renewed automatically; otherwise, owners receive an email 30, 15, and 1 day beforehand; without an owner, it goes to a fallback address. Groups that are not renewed are deleted and can be restored for 30 days. License: Entra ID P1 or P2 for the members, available but not necessarily assigned.

Policy for ownerless groups

Microsoft 365 admin center > Settings > Org settings > Services > Microsoft 365 Groups

Active members are asked weekly to become owners, and up to two can accept; otherwise, an administrator assigns one. Prerequisite according to Microsoft: for example, Microsoft 365 Business Premium, E3, or E5, or Entra ID P1 or P2.

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.

- Microsoft Learn: External sharing overview**
Models, levels, guests, security; October 25, 2026
learn.microsoft.com/de-de/sharepoint/external-sharing-overview
- Microsoft Learn: Manage sharing settings**
Sharing levels, settings, Anyone links; October 25, 2026
learn.microsoft.com/de-de/sharepoint/turn-external-sharing-on-o...
- Microsoft Learn: Change the sharing settings for a site**
Site level, default per site type; October 25, 2026
learn.microsoft.com/de-de/sharepoint/change-external-sharing-si...
- Microsoft Learn: How shareable links work (English)**
Link types; expiration of organization links only in English; October 25, 2026
learn.microsoft.com/en-us/sharepoint/shareable-links-anyone-spe...
- Microsoft Learn: Plan sharing and collaboration**
Sharing levels, default permission; October 25, 2026
learn.microsoft.com/de-de/sharepoint/collaboration-options
- Microsoft Learn: SharePoint and OneDrive integration with Entra B2B**
2026 changeover, end of the one-time passcode, FAQ; October 25, 2026
learn.microsoft.com/de-de/sharepoint/sharepoint-azureb2b-integr...
- Microsoft Learn: Configure external collaboration settings**
Guest access, invitations, domains; October 25, 2026
learn.microsoft.com/de-de/entra/external-id/external-collaborat...
- Microsoft Learn: Cross-tenant access**
Defaults, trust, P1 license; October 25, 2026
learn.microsoft.com/de-de/entra/external-id/cross-tenant-access...
- Microsoft Learn: B2B direct connect overview**
Shared channels, blocked by default; October 25, 2026
learn.microsoft.com/de-de/entra/external-id/b2b-direct-connect-...
- Microsoft Learn: MFA for B2B guest users**
Prerequisites, resource tenant; October 25, 2026
learn.microsoft.com/de-de/entra/external-id/b2b-tutorial-requir...
- Microsoft Learn: Guest access in Microsoft Teams**
Guest account, invitation, licensing; October 25, 2026
learn.microsoft.com/de-de/microsoftteams/guest-access
- Microsoft Learn: Turn Teams guest access on or off**
Teams admin center, features for guests; October 25, 2026
learn.microsoft.com/de-de/microsoftteams/set-up-guests
- Microsoft Learn: External access in Teams**
Domains, unmanaged accounts; October 25, 2026
learn.microsoft.com/de-de/microsoftteams/trusted-organizations-...
- Microsoft Learn: Guest access in Microsoft 365 groups**
Default, org settings; October 25, 2026
learn.microsoft.com/de-de/microsoft-365/admin/create-groups/man...
- Microsoft Learn: Labels for groups and sites**
Settings, enablement, management; October 25, 2026
learn.microsoft.com/de-de/purview/sensitivity-labels-teams-grou...
- Microsoft Learn: Labels for groups in Entra ID**
License, EnableMIPLabels; October 25, 2026
learn.microsoft.com/de-de/entra/identity/users/groups-assign-se...
- Microsoft Learn: Purview service description**
Labels, authentication context; October 25, 2026
learn.microsoft.com/de-de/office365/servicedescriptions/microso...
- Microsoft Learn: Guest access with access reviews**
Prerequisites, automatic removal; October 25, 2026
learn.microsoft.com/de-de/entra/id-governance/manage-guest-acce...

- | | |
|--|---|
| <p>19 Microsoft Learn: ID Governance, licensing for guests
Add-on, features without add-on, FAQ; October 25, 2026
learn.microsoft.com/de-de/entra/id-governance/microsoft-entra-i...</p> <p>21 Microsoft Learn: SharePoint Advanced Management
Prerequisites: base subscriptions, Copilot, Plan 1; October 25, 2026
learn.microsoft.com/de-de/sharepoint/sharepoint-advanced-manage...</p> <p>23 Microsoft Learn: Expiration policy for groups
License, renewal, notifications; October 25, 2026
learn.microsoft.com/de-de/entra/identity/users/groups-lifecycle</p> <p>25 NISG 2026, BGBl. I No. 94/2025 (RIS)
§§ 24 to 26, 32, 51; version as of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...</p> <p>27 Implementing Regulation (EU) 2024/2690
Annex points 11.1, 11.2.2(d), 11.2.3
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/deu</p> | <p>20 Microsoft Learn: Data access governance reports
Report types, frequency, E5; October 25, 2026
learn.microsoft.com/de-de/sharepoint/data-access-governance-rep...</p> <p>22 Microsoft Learn: Site sharing report
Running the report, CSV format; October 25, 2026
learn.microsoft.com/de-de/sharepoint/sharing-reports</p> <p>24 Microsoft Learn: Ownerless groups and teams
Prerequisites, setup, process; October 25, 2026
learn.microsoft.com/de-de/microsoft-365/admin/create-groups/own...</p> <p>26 NISV 2026, BGBl. II No. 290/2026 (RIS)
§§ 2 and 9; October 25, 2026
www.ris.bka.gv.at/eli/bgb/II/2026/290</p> <p>28 GDPR, Regulation (EU) 2016/679
Art. 32(1)(b) and (d) and (2)
eur-lex.europa.eu/eli/reg/2016/679/oj/deu</p> |
|--|---|