External sharing: who outside your organization can open your files today?

This month, make Specific people the default sharing link, turn Anyone links off or limit them to view-only links that expire within 30 days, and allow external sharing only on the sites, teams and shared drives set up for it. Then run the oversharing reports every quarter and fix the broadest exposure first: Anyone links, sites open to everyone in the organization, and guests nobody owns.

Reviewed
5 Nov 2026

Next review
5 Dec 2026

Version
1.0

Written for
IT, security and data protection leads in EU organizations on Microsoft 365 or Google Workspace who work with customers, partners and freelancers

Latest version
sheets.einblick.dev/external-sharing/

If you only do five things

1. **Make Specific people the default link.**
   Set it with View permission, as CISA's SharePoint baseline requires[6]. Only the named recipients can open it, after signing in, so a forwarded link is useless to anyone else[3]. In Google Drive, make new files private to their owner[7].
2. **Turn Anyone links off, or fence them in.**
   Anyone links need no sign-in, so nobody can tell who opened the file[3]. If you keep them, make them view-only, expire them within 30 days[6] and allow them only on sites that need them. Turning them off or shortening the expiry also affects existing links[1,2], so warn owners first. In Google, turn off "anyone with the link" for units that share externally[7].
3. **Share outside only from places built for it.**
   Keep sensitive sites internal and give each partner or project its own site or team; only SharePoint admins can change a site's sharing setting[2]. In Google, allow external sharing only in an empty organizational unit that holds a shared drive for external work[20].
4. **Limit sharing to approved people and domains.**
   Let only a security group share externally, and only with partner domains[1]. The domain list skips people who already have a guest account[6], so remove guests from domains you no longer work with. Set the same list in Entra, which also covers Teams[4].
5. **Find what's overshared before Copilot or Gemini does.**
   Both can surface anything a user can already open, and nothing more[15,24]. Microsoft advises running the site permissions report quarterly and the sharing links and "Everyone except external users" reports monthly[8]. In Google, check Data Protection Insights for sensitive files anyone on the web can open[22].

Set up sharing in Microsoft 365

1. **Set the organization level.**
   In the SharePoint admin center under **Policies** > **Sharing**, choose New and existing guests, or Anyone only if you need it; OneDrive can only be the same or stricter[1]. Turn on guest access expiration (30 to 730 days) and cap People in your organization links (7 to 720 days)[5]; links already older than the cap stop working[3].
2. **Set each site.**
   Under **Active sites** > **Settings** > **More sharing settings**, set sensitive sites to Only people in your organization and limit partner sites to the partner's domain[2]. Check the root communication site: it defaults to Anyone[2].
3. **Lock the most sensitive sites.**
   Restricted access control limits a site to up to 10 groups. Nobody outside them can open it, even with a link, or find it through search and Copilot. Set it separately on channel sites; it doesn't cover external participants in shared channels[10]. It needs SharePoint Advanced Management (SAM), which comes with one Copilot license on an E plan, or as an add-on[9].
4. **Act on the reports.**
   Send site access reviews from the data access governance reports to the owners of the broadest sites[8]. On E5 without SAM, turn on data collection for the activity reports first[8]. Otherwise, search the audit log for `AnonymousLinkCreated` and `SecureLinkCreated`[12].

Teams, chat and other tenants

- **Use shared channels for partners on Microsoft 365.** B2B direct connect is blocked both ways by default and needs both tenants to allow it. Its participants have no account in your directory to forget; the channel owner manages them[17].
- **Work in a partner's channel stays with the partner.** Its files sit in the partner's SharePoint under the partner's retention, DLP and eDiscovery[16], and your tenant gets no audit logs of your users' activity there[17]. Allow outbound direct connect only for named groups.
- **Set cross-tenant defaults.** B2B collaboration is open to every Entra tenant, and their MFA isn't trusted[18]. Add key partners and trust their MFA if they enforce it. Limit Teams chat to named domains, as the cloud configuration sheet explains.

If you run Google Workspace

- **Allowlist partner domains.** CISA's baseline restricts sharing to allowlisted domains, warns before sharing elsewhere and blocks moving files to other organizations' shared drives[7]. An allowlist also blocks personal Google accounts, such as freelancers' Gmail[23].
- **Allow visitors only from trusted domains.** Visitor sharing, for people without Google accounts, can be open to anyone or limited to trusted domains[20].
- **Restrict Chat too.** Check **Only allow this for allowlisted domains**. Turning external chat off later doesn't remove outsiders from existing chats and spaces[21].

- **Block exits through other tenants.** Tenant restrictions v2 stops users signing in to other tenants with outside accounts on your devices. Enforced through Windows, it can also block Anyone links and anonymous Teams meetings there (in preview)[19].

What you can skip

- **Restricted SharePoint Search.** It isn't a security boundary, holds at most 100 sites and can't be newly turned on since 31 July 2026[11]. Use restricted access control, or Restricted Content Discovery from the DLP sheet.
- **A sharing audit tool before the built-in reports.** SAM comes with a Copilot license on E plans, and E5 alone gets the activity reports[9,8].
- **Turning external sharing off everywhere.** Partners still need the files. A partner site can be audited and revoked; an email attachment can't.

Mistakes that cost the most

- **Using the site sharing report to find Anyone links.** It leaves them out[14]. Search the audit log for `AnonymousLinkCreated`[12], which keeps only 180 days of records without E5[13].
- **Expecting guest expiration to cover old guests.** It skips guests added before you turned it on[5]; review those per the joiners and leavers sheet.
- **Removing a partner from the channel but not the files.** Access granted to a file through SharePoint sharing stays after the person leaves[16].

What changed in 2026

- **Every named external share creates a guest.** Since July 2026, Entra B2B integration is permanent for SharePoint and OneDrive in commercial tenants[4]. If only admins and Guest Inviters may invite, as the cloud configuration sheet advises, others can share only with existing guests[1].
- **SharePoint one-time passcodes are retiring.** From October 2026, outsiders without a matching guest account lose access to Specific people links. Create the guest or reshare one item to restore access[4].
- **Google Workspace has guest accounts.** Since April 2026, inviting someone not on Workspace to Chat creates one, and by default everyone who can chat externally can invite. The Workspace Guests unit has its own security defaults, not your root ones, so apply 2-Step Verification there[23].

What this looks like at your size

Small team, no security staff

- Set the default link, Anyone limits and guest expiration in one sitting.
- Give each customer or freelancer one site or team, and remove it when the work ends.
- Each quarter, export the audit log's sharing events and remove links and guests nobody can explain.

Growing, with IT or security staff

- Run the data access governance reports monthly and send reviews to owners of the broadest sites.
- Put HR, finance and board sites behind restricted access control.
- Set up B2B direct connect and MFA trust with your biggest partners.

Enterprise or regulated

- Set sharing per sensitivity level with container labels, and alert when a site's label is lowered.
- Enforce tenant restrictions v2, and pilot its Windows option (in preview).
- Record each partner's setup and owner in the supplier list (see the third-party risk sheet).

Version history

5 Nov 2026, version 1.0	Published after a copy edit and a source-by-source fact check, which added warnings where a setting breaks existing links or guests and narrowed 8 statements to what the sources say.

Sources

1. Manage sharing settings for SharePoint and OneDrive. Microsoft Learn, 30 Jun 2026. learn.microsoft.com
2. Change the sharing settings for a site. Microsoft Learn, 7 May 2026. learn.microsoft.com
3. How shareable links work in OneDrive and SharePoint. Microsoft Learn, 12 Aug 2026. learn.microsoft.com
4. Entra B2B integration for SharePoint and OneDrive. Microsoft Learn, 18 Sep 2026. learn.microsoft.com
5. Set-SPOTenant. Microsoft Learn, 19 Oct 2026. learn.microsoft.com
6. CISA M365 Secure Configuration Baseline for SharePoint and OneDrive. CISA (ScubaGear), ScubaGear v2.0.0, Oct 2026. github.com
7. CISA Google Workspace Baseline for Google Drive and Docs. CISA (ScubaGoggles), ScubaGoggles v1.1.0, Oct 2026. github.com
8. Data access governance reports for SharePoint sites. Microsoft Learn, 9 Jul 2026. learn.microsoft.com
9. Prerequisites for SharePoint Advanced Management. Microsoft Learn, 30 Jun 2026. learn.microsoft.com
10. Restrict SharePoint site access with groups. Microsoft Learn, 30 Jul 2026. learn.microsoft.com
11. Restricted SharePoint Search. Microsoft Learn, 6 Jul 2026. learn.microsoft.com
12. Use sharing auditing in the audit log. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
13. Manage audit log retention policies. Microsoft Learn, 19 Jun 2026. learn.microsoft.com
14. Report on file and folder sharing in a SharePoint site. Microsoft Learn, 7 May 2026. learn.microsoft.com
15. Data, Privacy, and Security for Microsoft Copilot. Microsoft Learn, 9 Jul 2026. learn.microsoft.com
16. Shared channels in Microsoft Teams. Microsoft Learn, 9 Feb 2025. learn.microsoft.com
17. B2B direct connect overview. Microsoft Learn, 24 Apr 2026. learn.microsoft.com
18. Cross-tenant access overview. Microsoft Learn, 28 Mar 2025. learn.microsoft.com
19. Configure tenant restrictions. Microsoft Learn, 20 Mar 2026. learn.microsoft.com
20. Manage external sharing for your organization. Google Workspace Admin Help, updated 26 Oct 2026. knowledge.workspace.google.com
21. Control external Chat and spaces chat options. Google Workspace Admin Help, updated 26 Oct 2026. knowledge.workspace.google.com
22. DLP Data Protection Insights reports. Google Workspace Admin Help, updated 26 Oct 2026. knowledge.workspace.google.com
23. Introducing guest accounts. Google Workspace Updates, 30 Mar 2026. workspaceupdates.googleblog.com
24. Generative AI in Google Workspace Privacy Hub. Google Workspace Admin Help, updated 6 Oct 2026. knowledge.workspace.google.com