Rolling out a white-label, read-only Microsoft 365 sharing review: an MSP checklist

For MSPs evaluating or offering a white-labeled, read-only review of who can open what in a client's Microsoft 365 tenant. Free, no sign-up. Most of it applies whichever vendor you use, including none.

Clients are asking "Is Copilot safe to turn on?" The honest starting point is Microsoft's own: Copilot "only surfaces organizational data to which individual users have at least view permissions." [1] So the work is about permissions: Anyone links, sites open to the whole company, stale guests, and too many admins. A read-only review can map that for you. This checklist covers what to settle before you put your name on one.

Tell us what's missing at hello@truenorthdatashield.com. If you run these reviews already, you'll spot gaps we haven't.

1. Scoping

- [ ] Which clients fit. A review like this needs the client on Microsoft 365, with SharePoint, OneDrive and Teams in use. It is most useful before a Copilot pilot, before a renewal or questionnaire, or after staff or vendor turnover. Ask the client whether they plan to use Copilot; don't assume.
- [ ] What is in scope, in writing: sharing links (including Anyone links and expiry), sites and items shared company-wide, direct external shares, guests and their last sign-in, admin roles, and tenant-level sharing settings.
- [ ] What is out of scope, in writing: MFA, backups, endpoint protection, email security, mailbox and chat content, and what staff upload to outside AI tools. Name these so nobody assumes they were checked.
- [ ] What the client's licensing allows on their own. Microsoft's Data access governance reports and Restricted Content Discovery need SharePoint Advanced Management, and Microsoft's prerequisites list enterprise base plans, not the Business plans most small clients use. [2] The inactive guest report needs Entra ID Governance or Entra Suite. [3] This affects what the client could check without a tool, and what you can offer as follow-up.
- [ ] Who at the client owns the findings and will approve changes.

2. Client consent and authorization

- [ ] A written authorization from the client before any access is requested: what will be reviewed, by whom (you, and the vendor behind the white label), for how long, and how access ends.
- [ ] Be upfront that a third-party vendor does the scanning, even if the report carries your name. Clients often have to list vendors with access on their own questionnaires.
- [ ] The right person approves. Microsoft notes that apps needing Microsoft Graph application permissions require Global Administrator approval; the Application Administrator role can't grant those. [4] Find out whether your vendor uses application or delegated permissions.
- [ ] The client knows what they'll see. An admin consent prompt shows the app name, the publisher (or "Unverified" if the publisher isn't verified), and the list of permissions, under "Accept for your organization." [5] Walk them through it before the link arrives.

3. Read-only app consent: what you're actually granting

- [ ] Get the exact list of Microsoft Graph permissions from the vendor and read each one in Microsoft's permissions reference. [6] Every permission should be a read permission.
- [ ] Understand how broad "read" can be. For example, Microsoft describes Sites.Read.All as allowing an app "to read documents and list items in all site collections." [6] A vendor's promise not to open file contents is a design and policy choice, not something that permission enforces. Ask how they enforce it and whether that is in their written terms.

- [ ] After consent, check what was granted: Microsoft Entra admin center > **Entra ID** > **Enterprise apps** > **All applications** > select the app > **Permissions** > **Admin consent** tab. [7]
- [ ] Know how to remove it, and tell the client: same path, **Properties** > **Delete**. This needs Cloud Application Administrator, Application Administrator, or app owner. A deleted enterprise app sits in the recycle bin for 30 days and can be restored in that window. [8]
- [ ] Decide when access ends: right after the review, or kept for a scheduled re-check. Put that in the authorization.

4. Data handling

- [ ] What the vendor collects. Sharing metadata such as file names, paths, link types and who has access is still sensitive. A file name like "Payroll 2026.xlsx" tells a story by itself.
- [ ] Where it is stored, who at the vendor can see it, how long it is kept, and how it is deleted. Get these in writing, and check the vendor's data processing terms and subprocessor list.
- [ ] How reports reach you and the client. Avoid passing reports full of file names around as open email attachments if a better option exists.
- [ ] Your own client contracts. Some require notice or approval before a new subprocessor touches client data.

5. Report branding

- [ ] Review a sample report before you sell it. Check that the findings are ranked, readable by a business owner, and give recommendations, not just raw lists.
- [ ] Check every place the vendor's name may still appear: the consent prompt (it shows the app's registered name and publisher [5]), the enterprise app name in the client's tenant, emails, and report footers. Tell clients ahead of time so it doesn't look like a surprise.
- [ ] Keep honest disclaimers in the branded report: read-only, recommendations only, and not legal or insurance advice.

6. Delivery

- [ ] Agree on timing with the vendor and quote the client a realistic window.
- [ ] Decide who presents the findings, and do it in a short walkthrough rather than just emailing a PDF.
- [ ] Remediation is a separate decision. A read-only review recommends; you or the client's team make the changes. Quote fixes separately and make them optional.
- [ ] Plan a re-check. Sharing drifts: new Anyone links and guests show up weeks after a cleanup.

7. The conversation with the client

- [ ] Lead with their question ("What would Copilot be able to see?" or "Who can open our files?"), not with a scare.
- [ ] Explain the method in one breath: the client's admin approves read-only access, the tool looks at who can open what, and nothing is changed.
- [ ] Say what it doesn't do: it doesn't fix anything, doesn't cover MFA or backups, and isn't legal or insurance advice.
- [ ] Set expectations: findings are normal in any tenant that has been in use for a few years. The point is a prioritized list.
- [ ] Don't use the report as a pressure tool. Many owners and MSPs are wary of scans built to sell. Let the findings speak, and let the client decide what to fix and when.

A short way to say it: "Copilot can show people anything they can already open. Before you turn it on, we'd like to run a read-only check of who can open what: links, guests, admins and sharing settings. Your admin approves it, nothing gets changed, and you get a short list of what to fix first. Whether and when you fix things is up to you."

About TrueNorth's MSP Partner offer

What the TrueNorth website says the MSP Partner offer includes (homepage and /msp-partners page, read October 16, 2026):

- White-label reports with your branding

- Onboarding links for multiple client tenants; each client's Microsoft 365 admin approves read-only access for their own tenant
- The client relationship stays with you, and you set the resale price
- Partner rates are shared by email on request; a call is optional

The site also lists the four Microsoft Graph permissions requested (Sites.Read.All, Directory.Read.All, AuditLog.Read.All, SharePointTenantSettings.Read.All) and says access can be removed by deleting the enterprise application in Microsoft Entra ID. Before you commit, ask us in writing about the items in sections 2 to 5: whether the permissions are application or delegated, whether the app is publisher verified, which names your clients will see on the consent prompt and in their enterprise app list, whether file contents are ever read or downloaded, and where data is stored and for how long. We'd rather answer it than have you assume.

What this checklist does not cover. It doesn't cover MFA, backups, or what staff upload to ChatGPT or other outside AI tools. Those matter too, for your clients and for your own tenant. Microsoft says an account is 99.9% less likely to be compromised with MFA turned on. [9]

Next step, if useful: see a sample report at **truenorthdatashield.com/sample-report**, or choose MSP Partner at **truenorthdatashield.com/get-started**. A call is optional.

Sources (all opened October 16, 2026)

1. Microsoft Learn, Data, Privacy, and Security for Microsoft Copilot: https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy
2. Microsoft Learn, Prerequisites for SharePoint Advanced Management: https://learn.microsoft.com/en-us/sharepoint/sharepoint-advanced-management-prerequisites
3. Microsoft Learn, Monitor and clean up stale guest accounts: https://learn.microsoft.com/en-us/entra/identity/users/clean-up-stale-guest-accounts
4. Microsoft Learn, About administrator roles in the Microsoft 365 admin center: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles
5. Microsoft Learn, Consent experience for applications in Microsoft Entra ID: https://learn.microsoft.com/en-us/entra/identity-platform/application-consent-experience
6. Microsoft Learn, Microsoft Graph permissions reference: https://learn.microsoft.com/en-us/graph/permissions-reference
7. Microsoft Learn, Review permissions granted to enterprise applications: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions
8. Microsoft Learn, Delete an enterprise application: https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/delete-application-portal
9. Microsoft Learn, Best practices for Microsoft Entra roles: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices

---

TrueNorth Data Shield LLC • Veteran-owned • truenorthdatashield.com • hello@truenorthdatashield.com • 200 N Vineyard Blvd, Ste A325-231, Honolulu, HI 96817. Free to use and share. Microsoft 365, SharePoint, OneDrive, Teams, Entra and Copilot are trademarks of the Microsoft group of companies; TrueNorth Data Shield is not affiliated with or endorsed by Microsoft.