Who can access customer data?

A worksheet for answering the data access questions on cyber insurance applications and client security questionnaires. Free, no sign-up. Built for small businesses on Microsoft 365.

Please read first. This worksheet is general information, not legal or insurance advice. Requirements, wording and definitions vary by insurer, broker, policy and client. Always answer the exact questions on your own application or questionnaire, and ask your broker or carrier when a question is unclear. TrueNorth Data Shield LLC is not a law firm, insurance broker or carrier.

Why this is worth an hour

Most insurance applications and client questionnaires ask some version of "Who can access your customer data?" The answer matters more than it looks. As one broker's guide puts it: "The application is not a survey. It becomes part of the policy, and you sign a declaration that the answers are true." [1] (That guide is Canadian, and the rules where you are may differ, but the point holds: answer with evidence, not a guess.)

An honest "Partly, and here is our plan" is usually a better answer than a confident guess. This worksheet helps you find the facts in Microsoft 365 and write them down with a date.

How to use it

1. Work through Parts A to E with whoever manages Microsoft 365 (staff member, IT person or MSP).
2. For each row, write what you found, where you found it, and the date you checked. A screenshot or exported list is good evidence. Keep it with your application.
3. Use Part F to turn what you found into answers: **Yes**, **No**, or **Partly**, plus evidence and a date to fix.

Write "Not sure" when you don't know. Treat "Not sure" as "No" until someone checks.

Part A. Where customer data lives

List every place customer information is kept: client files, contracts, invoices, account numbers, contact lists. Include places outside Microsoft 365 too (accounting, CRM, practice or line-of-business software), even though this worksheet only walks you through Microsoft 365.

Where to look in Microsoft 365: SharePoint admin center > **Sites** > **Active sites**. Select a site and open the **Membership** tab to see its admins, owners, members and visitors. [2] For teams, the Teams admin center > **Teams** > **Manage teams** shows members, owners, guests and whether each team is public or private. [3]

Location (site, team, folder, app)	What customer data is there	Business owner	Who can open it (group or names)	Shared outside the company? (Y/N/Not sure)	Checked on (date)

Part B. Who has admin access

Admins can usually reach almost everything. Microsoft says Global Administrators "essentially have unrestricted access" and recommends fewer than five of them. [4]

Where to look:

- Microsoft 365 admin center > **Roles** > **Role assignments**. Select a role to see who holds it, or use **Export admin list** for the full list. [5]
- Microsoft 365 admin center > **Settings** > **Partner relationships** lists IT partners connected to your tenant. [6]
- Outside apps that can read your data: Microsoft Entra admin center > **Entra ID** > **Enterprise apps** > **All applications** > select the app > **Permissions**. [7]

Account	Role (for example Global Administrator)	Named person, shared account, or outside company	Still needs it? (Y/N)	Action and date

Number of Global Administrators today: _____ Checked on: _____

Outside app or partner with access	What it can read	Who approved it	Still in use? (Y/N)	Action and date

Part C. Guests and other outside people

Guests are people outside your company who were given an account in your tenant, often through Teams or SharePoint sharing.

Where to look: Microsoft 365 admin center > **Users** > **Guest users**. You can remove a guest's access there. [8] If you have Microsoft Entra ID Governance or Entra Suite, the inactive guest report (Entra admin center > **ID Governance** > **Dashboard** > **View inactive guests**) uses 90 days without activity as its default. [9]

Guest (name or email)	Company	Why they have access	Still needed? (Y/N)	Action and date

Total guests today: _____ Removed or still to review: _____

Part D. External sharing settings

These settings control how files can be shared outside the company from now on.

Where to look: SharePoint admin center > **Policies** > **Sharing**. [10] For a single site: **Sites** > **Active sites** > select the site > **Settings** > **More sharing settings**. [11]

Setting	What it is set to today	Is that a deliberate choice? (Y/N)	Evidence (screenshot name)	Checked on
SharePoint external sharing level (Anyone / New and existing guests / Existing guests / Only people in your organization)				
OneDrive external sharing level				
Anyone links must expire after (days), if Anyone is allowed				
Anyone links limited to View, if Anyone is allowed				
Default link type under File and folder links				

Setting	What it is set to today	Is that a deliberate choice? (Y/N)	Evidence (screenshot name)	Checked on
Guest access expires after (days)				
Sharing limited to specific domains				
Sites holding customer data set stricter than the default				

Part E. Anyone links and files already shared outside

Settings control new sharing. This part is about what is already out there. An "Anyone" link works for whoever has it, without signing in, so a forwarded link is effectively public. Microsoft notes that with Anyone links "you can't track who has access." [10]

Where to look: Microsoft Purview portal > **Audit** > **Search**. Under Activities, choose **Sharing and access request activities**, pick a date range, search, and export. Filter for events such as AnonymousLinkCreated (an Anyone link was made) and SharingInvitationCreated. [12] Audit search only reaches back so far: Audit (Standard) keeps records for 180 days by default, so older links won't show up this way. [13]

File or folder	Location	Link type (Anyone / specific outside people)	Shared with	Still needed? (Y/N)	Action and date

Part F. Turning what you found into answers

The questions below are common examples, not quoted from any particular insurer or client. Match each one to the actual wording on your form.

Example question	Answer (Yes / No / Partly)	Evidence (which Part, file name, date)	If Partly or No: what you will change, and by when
Is access to customer data limited to people who need it for their job?			
How many people have administrative access?			
Do any outside parties (vendors, IT providers, guests) have access to your systems or data?			
Do you review user and guest access on a schedule? How often?			
Can files be shared with people outside the company? Is that restricted?			
Are public or unauthenticated sharing links allowed?			
Where is customer data stored?			

What a "Partly" answer can look like (example only): "Partly. Administrative access is limited to three named people as of [date]. Two older guest accounts and four Anyone links to client folders were found and are being removed, with completion expected by [date]."

Keep this worksheet and your evidence with a copy of what you submitted. Next year's renewal will be faster.

What this worksheet does not cover. It doesn't cover MFA, backups, or what staff upload to ChatGPT or other outside AI tools. Those matter too, and insurance applications often ask about them directly. Microsoft says an account is 99.9% less likely to be compromised with MFA turned on. [4] It also doesn't cover email security, device protection, or systems outside Microsoft 365.

Want a dated record of the Microsoft 365 part? TrueNorth Data Shield runs a read-only review of sharing links, guests, admin roles and sharing settings, and gives you a report with recommendations you can keep as evidence. It doesn't change anything, and it isn't legal or insurance advice. See a sample report at **truenorthdatashield.com/sample-report**, or start at **truenorthdatashield.com/get-started**. A call is optional.

Sources (all opened October 16, 2026)

1. Privateer, Cyber insurance application guide (PDF, no date shown): https://privateer.ca/assets/downloads/guides/cyber-insurance-application.pdf
2. Microsoft Learn, Manage sites in the SharePoint admin center: https://learn.microsoft.com/en-us/sharepoint/manage-sites-in-new-admin-center
3. Microsoft Learn, Manage teams in the Microsoft Teams admin center: https://learn.microsoft.com/en-us/microsoftteams/manage-teams-in-modern-portal
4. Microsoft Learn, Best practices for Microsoft Entra roles: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices
5. Microsoft Learn, Assign admin roles in the Microsoft 365 admin center: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/assign-admin-roles
6. Microsoft Learn, Add, change, or delete a subscription advisor partner (View your partner relationships): https://learn.microsoft.com/en-us/microsoft-365/admin/misc/add-partner
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, Guests in the Microsoft 365 admin center: https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-guest-users
9. Microsoft Learn, Monitor and clean up stale guest accounts: https://learn.microsoft.com/en-us/entra/identity/users/clean-up-stale-guest-accounts
10. Microsoft Learn, Manage sharing settings for SharePoint and OneDrive: https://learn.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off
11. Microsoft Learn, Change the sharing settings for a site: https://learn.microsoft.com/en-us/sharepoint/change-external-sharing-site
12. Microsoft Learn, Use sharing auditing in the audit log: https://learn.microsoft.com/en-us/purview/audit-log-sharing
13. Microsoft Learn, Manage audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies

---

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.