SharePoint Document Library Architecture

The Future Proof Plan to Secure Data Management

Provided by

TRUSTED BY THE WORLDS LEADING SECURITY VENDORS

CROWDSTRIKE Delinea netskope THREATLOCKER veeam Microsoft

Organisations don’t have a SharePoint problem. They have an access discipline problem.

Most environments grow organically - folders created on the fly, permissions granted directly to individuals, inheritance broken randomly, and “temporary access” that quietly becomes permanent. It works… until it doesn’t.

Now introduce AI.

If Microsoft 365 Copilot (or any AI capability) is enabled in a poorly governed tenant, it doesn’t magically understand intent - it simply surfaces whatever users technically have access to. If permissions are messy, AI will faithfully expose messy access at scale.

That’s not an AI risk. That’s a governance failure being amplified.

What We Are Doing

We are implementing a top-down, identity-driven access model across SharePoint and Entra ID that ensures:

- Access is controlled centrally through Entra ID groups, not granted directly to individuals.
- Permissions are applied at structured folder levels, starting from the top of the document library and cascading intentionally.
- Data Owners define who should access information, and IT enforces that access via group membership.
- Library-level permissions are locked down, preventing uncontrolled inheritance and accidental exposure.
- External sharing is controlled and isolated, reducing data sprawl.

In short: Access to documents is determined by who you are (role/team) - not by who happened to be added to a folder three years ago.

The Core Principle

If you don't have access to something today, AI shouldn't be able to surface it tomorrow.
This model ensures that when AI is enabled:

- Users only see content aligned to their role.
- Sensitive folders are not accidentally indexed for the wrong audiences.
- Information discovery is governed by deliberate access controls.
- AI becomes a productivity accelerator - not a compliance liability.

Problems This Fixes

- **Overexposure of Sensitive Information** - Removes ad-hoc user-level permissions that silently expand access over time.
- **"Permission Sprawl"** - Eliminates unmanaged inheritance and one-off sharing decisions that compound into risk.
- **AI Data Leakage Risk** - Prevents AI from surfacing documents users technically have access to but should never have retained.
- **Lack of Accountability** - Introduces clear Data Ownership - someone is responsible for each area of information.
- **Operational Inefficiency** - Streamlines onboarding and offboarding. Access changes happen once in Entra ID group membership - not across dozens of folders.

The Strategic Outcome

- Least privilege by design
- Predictable access structure
- Reduced audit and compliance risk
- AI readiness without fear
- Governance that scales with growth

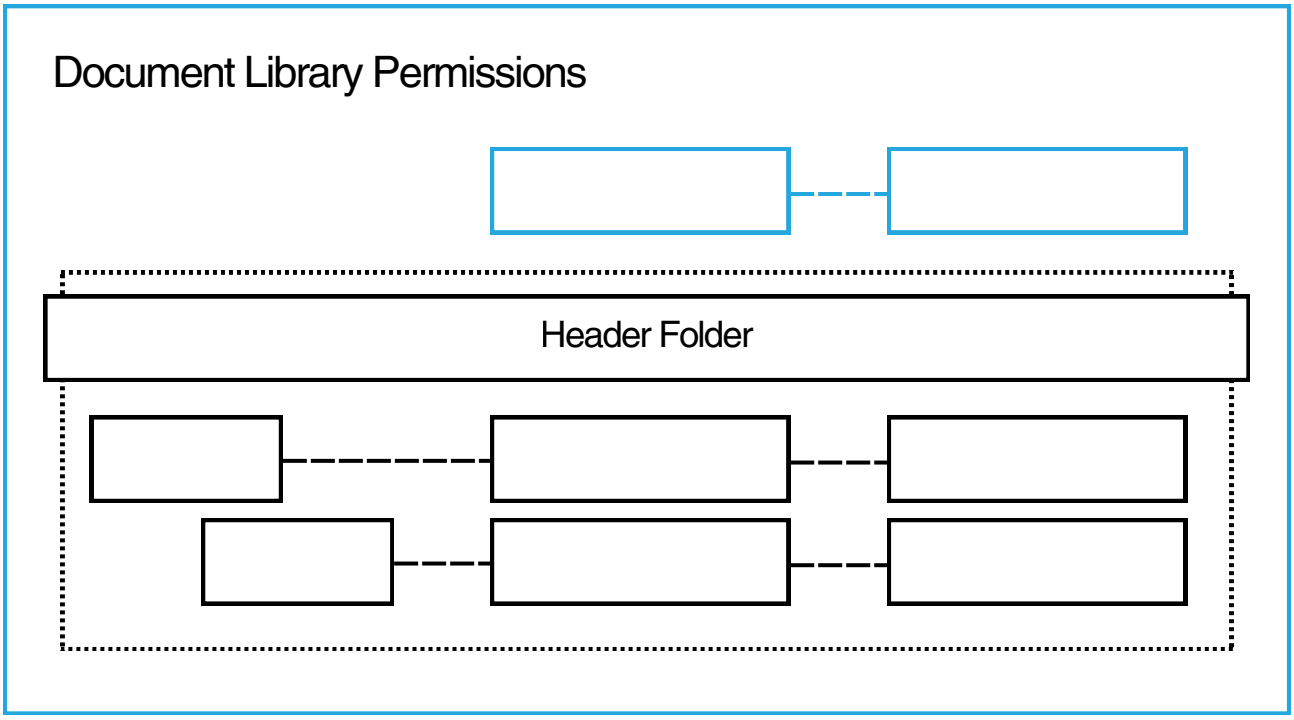
This isn't just about tidying up SharePoint. It's about ensuring that when AI turns on, your organisation isn't surprised by what it finds. And more importantly - neither are you.

Goal: A single source of truth in SharePoint where access is governed by Entra ID group membership, not random ad-hoc sharing.

Simple Architecture

- **One central SharePoint document library** (“File Server” / “Repository”) that becomes the governed home for working files, a single library to sync.
- **A 3-layer folder model** (Header → Level 2 → Level 3) where permissions are applied using Entra ID groups.
- **Data Owners** decide who gets access; IT implements via groups + folder permission application.

File Server - Document Library



Step by Step Build

#1 Lock down the library first

Why: Library-level permissions affect everything. If you get this wrong, every "granular" folder permission becomes theatre.

1. Go to the document library (your central repository).
2. Open Settings (cog) → More Library Settings → Permissions for this document library.
3. Ensure inheritance is broken and the library permission set is minimal (admin-only control). The doc explicitly warns: do not adjust library-level permissions once set, because it can negate folder-level controls.

Outcome: Only admin-level control exists at the library root; everything else is controlled at folder level.

#2 Define your permission levels *(keep it boring and consistent)*

Create three permission levels for the library and use them everywhere (names can be yours, but keep 3 tiers):

1. **Read:** users can see/navigate and read contents, but can't create subfolders.
2. **Write:** users can create/edit/delete in the folder, but can't share to people without access.
3. **Full:** "data owner" control at level 2/3 where they manage items and can manage sharing for their area. This means they can share information with people freely, not governed by Entra ID group Structure. Only use if needed. Otherwise, ask them to download the file to their OneDrive and Share if needed.

Rule of thumb: apply access hierarchically; highest privilege wins.

Note: If folders have folders or files in them, do not set the as read only if you want people to be able to sync the folders in their file explorer. Windows needs to be able to download a file to sync it.

#3 Design the folder structure with Data Owners *(before you touch permissions)*

Create a (or use supplied) spreadsheet that lists:

- **Header folder (department)**
- Level 2 folder
- Level 3 folder (optional)
- Data Owner role/group
- Read/Write/Full access groups needed

Establish Data Owners per header folder (one accountable "owner of the data", not "everyone owns it").

Keep the structure to max 3 layers to avoid a permissions labyrinth nobody understands later.

Outcome: A clear structure and accountability model before you create 400 groups you'll regret.

Continued on next page...

#4 Standardise Entra ID group naming *(so future-you doesn't hate past-you)*

Create EntraID Security Groups that follow a predictable pattern:

Header folders (only "READ" at the header level)
- FSA-<HEADER>-READ

Level 2 folders
- FSA-<HEADER>-<FolderName>-READ (File Explorer can't sync if contains files)
- FSA-<HEADER>-<FolderName>-WRITE
- FSA-<HEADER>-<FolderName>-FULL

Level 3 folders
- FSA-<HEADER>-<FolderName>-<FolderName>-READ (File Explorer can't sync if contains files)
- FSA-<HEADER>-<FolderName>-<FolderName>-WRITE
- FSA-<HEADER>-<FolderName>-<FolderName>-FULL

Key operating principle: for scalability, permissions are applied to folders via Entra ID groups, not individuals.

#5 Build "ROLE" and "TEAM" groups in Entra ID *(the scalable part)*

1. Create ROLE groups (e.g., ROLE-CFO, ROLE-CEO, ROLE-CHRO) as people leave, you can replace with the new person, who then gains access to everything they need.
2. Create TEAM groups (e.g., TEAM-Finance, TEAM-Sales, TEAM-Board) and assign users accordingly.
    a. Create the via Dynamic user membership groups for the most scalable outcome.
3. Maintain access groups based on your spreadsheet (example patterns are shown in the doc).
4. Nest ROLE and TEAM groups into the relevant folder access groups (FSA groups), so onboarding is just "add user to TEAM/ROLE" and access flows automatically.

Outcome: You've separated identity management (ROLE/TEAM) from resource permissions (FSA), which is exactly how it should be.

#6 Apply folder permissions in SharePoint *(repeatable method)*

For each folder that needs unique permissions:

1. In the library, go to the folder → ellipsis (…) → Manage access.
2. Select More options → Advanced.
3. Click Stop inheriting permissions.
4. Remove access entries that shouldn't be there (e.g., inherited read at the wrong level).
5. Click Grant permissions.
6. Enter the relevant FSA group name, untick "share everything in this folder", show options, and disable email invites.
7. Select the matching permission level (Read/Write/Full).

Continued on next page...

#7 Critical rule: Header folders stay “READ”

Header folders (top-level department folders) should be READ only, with FULL applied only below that where the data owner’s working structure starts.

#8 Access methods
(help users actually use the library)

Users will access the governed repository via:

- SharePoint intranet navigation
- Teams (add a SharePoint library location into a Team tab by URL)
- Sync to File Explorer (sync what they need, not the entire universe)

#9 External sharing rule
(non-negotiable, unless you like incidents)

External sharing should be done via OneDrive, not directly from the central repository—copy/download to OneDrive and share with time limits.

#10 Migration + syncing safety notes
(aka “how to avoid self-inflicted pain”)

- Data Owners move content into the new structure once folders are ready, keeping only what’s needed.
- Syncing too much content can crush endpoints (and increases exposure if a device gets popped).


CORNERSTONE
CYBER