SharePoint Permission Review Checklist for Copilot

A practical planning tool for reducing oversharing, stale access, broken inheritance, and content exposure before Microsoft 365 Copilot is expanded across SharePoint.

Why this matters

Copilot respects Microsoft 365 permissions, but weak SharePoint permissions become easier to discover when users can ask questions across accessible content. Start with access, ownership, and source-of-truth cleanup before relying on prompt testing.

Organization		**Review date**	
Reviewer(s)		**Business area**	
Scope		**Target Copilot date**	

Use this checklist to

Identify high-risk sites, confirm ownership, review internal and external access, document exceptions, and build a cleanup plan.

Review priority

Start with HR, legal, finance, executive, regulated, customer, project, and policy content before lower-risk intranet pages.

Recommended cadence

Use this before Copilot rollout, after major migrations, during quarterly governance reviews, and when sensitive content libraries change.

Output

A scoped permission inventory, risk score, action plan, validation record, and approval trail for SharePoint and Microsoft 365 stakeholders.

Quick triage guide

Risk level	Typical signal	Recommended next move
High	Sensitive content, external sharing, broad groups, stale owners, or many unique permissions.	Pause broad rollout for that site. Assign an owner and clean access before validation testing.
Moderate	Active business content with some exceptions, unclear group purpose, or inherited migration permissions.	Review groups, simplify access, document exceptions, then retest with representative users.
Lower	Current content, active owners, simple groups, limited sharing, and clear lifecycle controls.	Confirm baseline reports and add the site to the recurring governance review cycle.

Step 1: Scope the Permission Review

Use this page to define which SharePoint sites, Teams-connected sites, hubs, libraries, and sensitive content areas need review before Copilot rollout or expansion.

Scope checklist

Done	Review	N/A	Checklist item	Notes / action
			Identify SharePoint sites, Teams-connected sites, hub sites, and document libraries in scope.	
			Prioritize sites that contain HR, legal, finance, executive, regulated, customer, contract, or project data.	
			Confirm the business owner for each site or library. The owner must be able to approve access changes.	
			Confirm Microsoft 365 group owners and SharePoint site owners are current, active, and accountable.	
			Collect current permission reports, sharing reports, guest user lists, and external sharing settings.	
			List known problem areas, including old project sites, inherited file shares, legacy folders, and unmanaged Teams.	
			Agree which access patterns should be removed, simplified, archived, restructured, or left unchanged.	
			Define who performs the cleanup, who validates the results, and who signs off on the final state.	

Priority site inventory

Site / library	Business owner	Content type	External users?	Sensitive content?	Main permission concern	Next action

Step 2: Review Owners, Groups, Members, and Broken Inheritance

Copilot readiness improves when access is simple, role-based, and owned. Use this section to remove stale access, reduce individual exceptions, and document unique permissions.

Ownership and permission structure checklist

Done	Review	N/A	Checklist item	Notes / action
			Each site has at least two active business or technical owners who understand the content and access model.	
			Stale site owners, group owners, and inactive administrators have been removed or replaced.	
			Members, visitors, and owners groups align with the current business purpose of the site.	
			Access is assigned through Microsoft 365 groups, Entra ID security groups, or SharePoint groups wherever possible.	
			Individual user exceptions are reviewed, justified, and documented. Unneeded exceptions are removed.	
			Everyone, Everyone except external users, company-wide groups, and broad department groups are reviewed for risk.	
			Members with edit rights are limited to users who truly need to create, modify, or manage content.	
			Visitors with read access are appropriate for the site purpose and do not expose sensitive content.	
			Broken inheritance at the library, folder, and item level has been identified and documented.	
			Unique permissions are removed where possible or tied to a clear business reason and owner.	
			Permission changes match job roles, process ownership, and approved information architecture.	
			A baseline permission report is saved before and after cleanup.	

Permission exception notes

Site / library / folder	Exception	Business reason	Owner	Keep / remove / simplify	Due date

Step 3: Review External Sharing, Guests, Links, and Sensitive Content

External access and sharing links often create the largest practical exposure before Copilot rollout. Review them alongside sensitive content, labels, and lifecycle controls.

External sharing and sensitive content checklist

Done	Review	N/A	Checklist item	Notes / action
			Guest users are reviewed against active business need, current projects, and approved partner relationships.	
			Expired, duplicate, inactive, or unknown guests are removed or flagged for owner review.	
			Anonymous or Anyone links are removed, blocked, or limited where they are not explicitly approved.	
			Organization-wide links and broad sharing links are reviewed for sensitive libraries and high-value content.	
			Edit links are reviewed more carefully than view-only links, especially on policy, procedure, contract, and customer documents.	
			Folder-level external sharing is reviewed because it can quietly expose more content than intended.	
			External sharing settings are aligned with site purpose, tenant policy, and approved domain rules.	
			Libraries containing confidential, HR, legal, financial, regulated, or customer content are identified.	
			Sensitivity labels, retention labels, DLP policies, or records controls are noted where they apply.	
			Sensitive content stored in the wrong site, Team, folder, or library is marked for relocation or restructuring.	
			Old sensitive content is archived, removed, or assigned to an accountable owner before Copilot validation.	
			Content owners validate that the final permission model supports least-privilege access.	

External access review log

Site / library	Guest / link / domain	Current access	Risk	Owner decision	Action taken

Step 4: Validate Copilot Readiness After Cleanup

Permission cleanup is not finished until representative users validate what they can find. Use this section to test access, search behavior, and Copilot readiness assumptions after changes are made.

Copilot validation checklist

Done	Review	N/A	Checklist item	Notes / action
			Test with representative users from different roles, departments, and permission levels.	
			Confirm users can find the content they should use and cannot access restricted content.	
			Run SharePoint search checks for sensitive terms, project names, customer names, and policy titles.	
			Use sample Copilot prompts only after permission cleanup and search checks are complete.	
			Validate that duplicate, outdated, and conflicting documents are reduced or clearly marked.	
			Identify the source of truth for policies, procedures, templates, knowledge articles, and operational documents.	
			Improve titles, metadata, library structure, and page ownership where findability is weak.	
			Confirm archived or retired content is no longer presented as active guidance.	
			Document exceptions that remain and assign a review date for each exception.	
			Save final permission, sharing, and validation evidence for governance review.	

Permission risk scorecard

Governance category	Score 1-5	Main evidence	Priority action
Ownership			
Broad internal access			
Guest and external sharing			
Sharing links			
Broken inheritance			
Sensitive content exposure			
Duplicate or stale content			
Source-of-truth clarity			
Total score			

Score guide: 1 = controlled and documented. 3 = some gaps or exceptions. 5 = high exposure or unclear ownership. Prioritize categories with the highest score first.

Step 5: Build the Cleanup Plan and Sign-Off Record

Use the final page to turn the review into a practical action plan. Permission cleanup should have owners, dates, validation steps, and a repeatable governance rhythm.

30 / 60 / 90-day cleanup plan

Timeframe	Recommended focus	Owner	Due date	Status
First 30 days	Inventory priority sites, confirm owners, remove urgent risky links, review guests, and clean the highest-risk sensitive libraries.			
31-60 days	Simplify groups, reduce broken inheritance, align labels and policies, archive stale content, and document remaining exceptions.			
61-90 days	Validate with role-based users, update governance standards, schedule recurring reviews, and save evidence for stakeholders.			

Decision and approval log

Decision	Site / library	Approval owner	Date	Notes

Sign-off

Role	Name	Signature / approval	Date

Need help with permission cleanup before Copilot?

dataBridge helps organizations assess SharePoint permissions, governance, external sharing, and Copilot readiness before Microsoft 365 Copilot expands content discovery. Visit getsharepoint.com/contact-us to start a review.

Related dataBridge resources

Copilot Readiness for SharePoint	SharePoint Permission Review Checklist
SharePoint Permissions Guide	SharePoint Governance Guide