ShareGate

SHAREGATE MCP

Starter Prompt Pack

Created by **Jim Ehrenberg** of SharePoint Pros

Contents

01

REDUCE COSTS

License waste recovery

USE CASE

You need to find paid licenses sitting with users who aren't using them—the clearest dollar-denominated win in a governance review. Run this for a cost-recovery conversation with finance or leadership, at renewal time, or as part of a quarterly license true-up. This is the prompt that turns a governance finding into a budget number, so the framing matters: real reclaimable dollars, not raw counts.

THE PROMPT

INSTRUCTIONS

- Write for a non-technical reader, with one short technical line per entry for admins (UPN, license SKU, last activity). Present findings in a single table. Use bullets only for risks and steps.
- Rank by highest reclaimable cost, top 10 only (note how many remain and give the total monthly figure). If no inactive users hold paid licenses, say so as a positive finding rather than an empty table.

- Count only genuinely paid SKUs. Exclude free/trial products (Fabric Free, Power Automate/Apps trials, Windows Store) from the dollar total and say so. A high-severity "unallocated license" count can resolve to $0 reclaimable. Use list prices as a labeled estimate only. A seat may not be reclaimable mid-term. Separate truly inactive users from light users or those on leave; don't reclaim on inactivity alone without a human check. State data currency (last completed crawl, not live status).
- For each finding, give a specific action tied to that user, grouped by urgency: immediate (clearly inactive users on high-cost E5/Copilot seats to reclaim after a quick confirmation), short-term (lower-cost or ambiguous seats to review with the manager), ongoing (recurring true-up + inactivity-based reclaim policy).
- Cite only official Microsoft Learn or ShareGate docs (no invented URLs). If results are extensive, summarize and point to Protect's reports and export for the full CSV. End with one logical follow-up, such as reconciling Copilot-eligible users against those actually assigned a Copilot license.

PARAMETERS · OPTIONAL SWAPS

Inactivity window default is 90 days.

`STRICTER` → *"...inactive 180+ days, for a conservative reclaim list."*

License focus all paid SKUs by default.

`COPILOT ONLY` → *"...only users holding a Microsoft Copilot license."*

`PREMIUM ONLY` → *"...only E5 and Copilot seats, skip E3."*

Rate basis list price by default.

`CONTRACTED RATES` → *"...apply our contracted per-seat rates instead of list price: [E3 $X, E5 $Y, Copilot $Z]."*

02

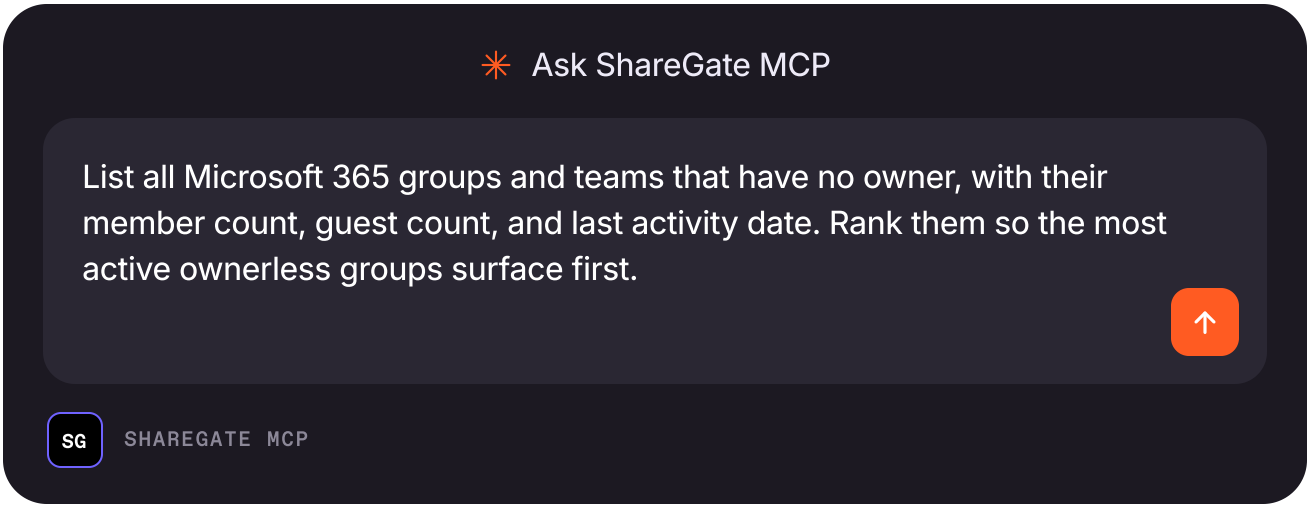
CONTROL SPRAWL

Ownerless groups & teams

USE CASE

You're cleaning up your tenant and need to know which Groups, Teams, and sites are running with no one in charge before something breaks and there's no one to call. This prompt finds the Microsoft 365 groups and teams that nobody owns. An ownerless group is a governance blind spot: no one is accountable for who's a member, whether its content is still needed, or whether its sharing settings are safe. They pile up when employees leave and ownership is never reassigned. Run this as a routine sprawl check, before a migration, or whenever offboarding leaves groups stranded. Ownerless plus external-capable is the worst pairing — nobody is watching, and outsiders may still have a way in.

THE PROMPT



INSTRUCTIONS

- Write for a non-technical reader, with one short technical line per entry for admins (group name, member/guest counts, last activity, team vs. group). Present findings in a single table. Use bullets only for risks and steps.
- Rank highest-to-lowest risk, top 10 only (note how many remain). If none are ownerless, say so as a positive finding rather than an empty table.

- Score risk on activity, guests/external sharing, and membership size. A busy, guest-bearing group is urgent. A dormant empty one isn't. Don't flag an empty owner field alone, separate genuinely abandoned groups from mid-transition ones. Flag Copilot exposure where broad or external access applies. State data currency (timestamps reflect the last completed crawl, not live status).
- For each finding, give a specific action tied to that object, grouped by urgency: immediate (active/guest-bearing groups needing an owner now), short-term (dormant groups to reassign or decommission), ongoing (recurring checks + Entra expiration/ownership policy).
- Cite only official Microsoft Learn or ShareGate docs (no invented URLs). If results are extensive, summarize and point to Protect's reports and export for the full CSV.

PARAMETERS · OPTIONAL SWAPS

Workload focus Groups and teams together by default.

`TEAMS ONLY` → *"...only teams, skip groups without a team."*

Activity filter all ownerless groups by default.

`ACTIVE ONLY` → *"...only ownerless groups with activity in the last 90 days."*

`DEAD WEIGHT` → *"...only ownerless groups with no activity in 180+ days, for decommissioning."*

Exposure focus all ownerless groups by default.

`EXTERNAL-CAPABLE ONLY` → *"...only ownerless groups that also have guests or external sharing."*

03

CONTROL SPRAWL

Inactive & stale workspaces

USE CASE

You're staring down a new phase of your Copilot rollout and need to know which workspaces are wide open to everyone in the org. With this prompt, you can find the workspaces nobody uses anymore—sites, groups, and teams with no meaningful activity for months. Stale workspaces are dead weight that still consumes storage, still hold permissions, and still feed Copilot with outdated content. Run this for a monthly or quarterly lifecycle review, before a migration (so you don't carry junk across), or to build the archive-and-retire habit that keeps a tenant clean. Low urgency individually, high cumulative payoff.

THE PROMPT

INSTRUCTIONS

- Write for a non-technical reader. Convey that the workspace looks abandoned with one short technical line per entry for admins (workspace, type, owner, storage, last activity). Present findings in a single table. Use bullets only for risks and steps.
- Rank longest-inactive to most-recent, top 10 only (note how many remain and give total reclaimable storage). If no workspaces are inactive, say so as a positive finding rather than an empty table.

- Score risk on external sharing/guests, ownership, and storage size. A large, guest-bearing dead site outranks a small, empty one. Separate genuinely abandoned workspaces from intentionally archival ones (a reference site, a seasonal team between cycles). Don't recommend deletion on inactivity alone without owner confirmation. Flag Copilot exposure where stale content has broad or external access. State data currency (last completed crawl, not live status).
- For each finding, give a specific action tied to that workspace, grouped by urgency: immediate (stale workspaces with external sharing or guests to secure or archive now), short-term (ownerless or large stale workspaces to review with stakeholders), ongoing (recurring lifecycle review + archive/retention policy).
- Cite only official Microsoft Learn or ShareGate docs (no invented URLs). If results are extensive, summarize and point to Protect's reports and export for the full CSV. End with one logical follow-up, such as checking the sharing or guests on the largest stale workspace before archiving it.

PARAMETERS · OPTIONAL SWAPS

Inactivity window default is 90 days.

`STRICTER` → *"...inactive 180+ days, for a firm retirement list."*

`EARLY WARNING` → *"...inactive 60+ days, to catch sites going quiet sooner."*

Workload focus all workspace types by default.

`TEAMS ONLY` → *"...only inactive Teams."*

`SITES ONLY` → *"...only inactive SharePoint sites."*

Exposure focus all stale workspaces by default.

`RISKY ONLY` → *"...only stale workspaces that still have external sharing or guests."*

04

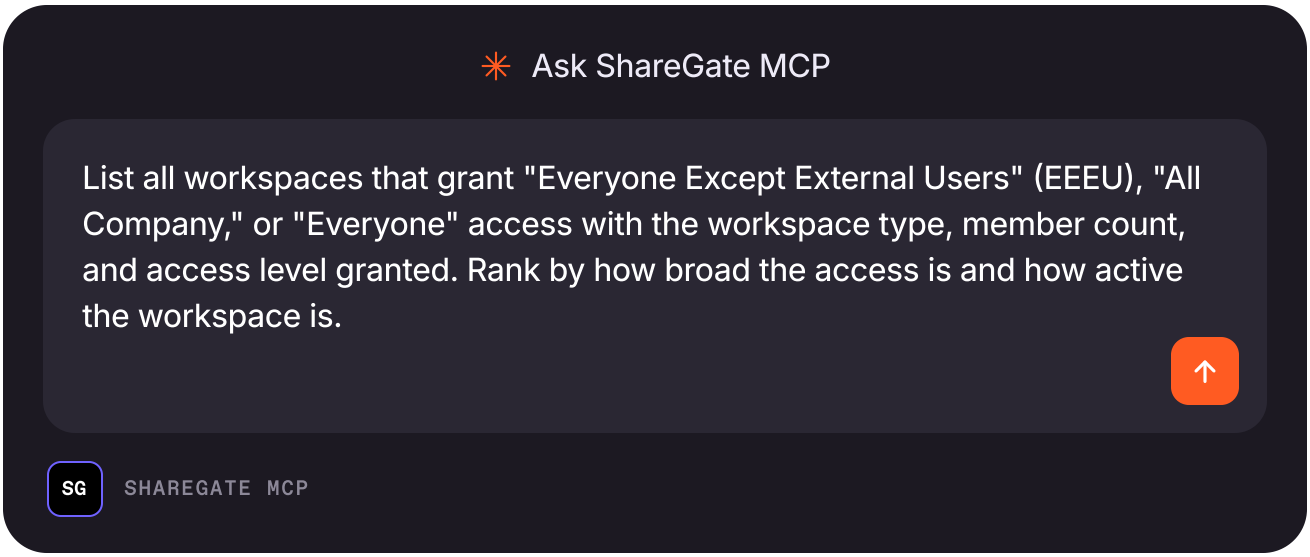
PREVENT OVERSHARING

Broad-access permissions (EEEU / All Company)

USE CASE

You need to find the workspaces that combine two amplifiers—public visibility inside the org and active external sharing—because that combination is where guests see things they shouldn't. This prompt surfaces workspaces with "Everyone Except External Users" (EEEU), "All Company," or "Everyone" access. These are silent oversharing: no link to revoke, no guest to remove, just a broad permission that quietly makes a site readable to the entire organization. Run this when hardening access before a Copilot rollout, during a least-privilege review, or whenever a site that should be team-scoped turns out to be company-wide. It's the structural counterpart to a sharing-link sweep. Links expose files, these grants expose whole workspaces.

THE PROMPT



INSTRUCTIONS

- Write for a non-technical reader. Convey that "everyone in the company can see this" plainly with one short technical line per entry for admins (workspace, access principal, access level). Present findings in a single table. Use bullets only for risks and steps.

- Rank highest-to-lowest risk, top 10 only (note how many remain). If no workspaces grant broad internal access, say so as a positive finding rather than an empty table.
- Score risk on access level (edit+ is worse than view), content sensitivity, and any external sharing. EEEU with edit on a finance site is far worse than EEEU view on a handbook. Separate intentional grants (all-staff intranet, announcements) from accidental ones (a project site that drifted company-wide). Flag Copilot exposure prominently—broad internal grants are a top Copilot risk, surfacing company-readable content to anyone who asks. State data currency (last completed crawl, not live status).
- For each finding, give a specific action tied to that workspace, grouped by urgency: immediate (edit-level broad grants on sensitive workspaces to tighten now), short-term (view-level grants to review with the owner for intent), ongoing (recurring broad-access review + least-privilege standard for new sites).
- Cite only official Microsoft Learn or ShareGate docs (no invented URLs). If results are extensive, summarize and point to Protect's reports and export for the full CSV. End with one logical follow-up, such as listing the members or sharing links on the highest-risk broad-access workspace.

PARAMETERS · OPTIONAL SWAPS

Grant type EEEU, All Company, and Everyone by default.

`EEEU ONLY` → *"...only 'Everyone Except External Users' grants."*

`ANONYMOUS-CAPABLE` → *"...include 'Everyone' grants that may reach external users."*

Access-level focus all levels by default.

`EDIT AND ABOVE` → *"...only grants at edit, contribute, or full-control, skip view-only."*

Workspace filter tenant-wide by default.

`SENSITIVE SCOPE` → *"...only workspaces holding client, finance, or HR content."*

05

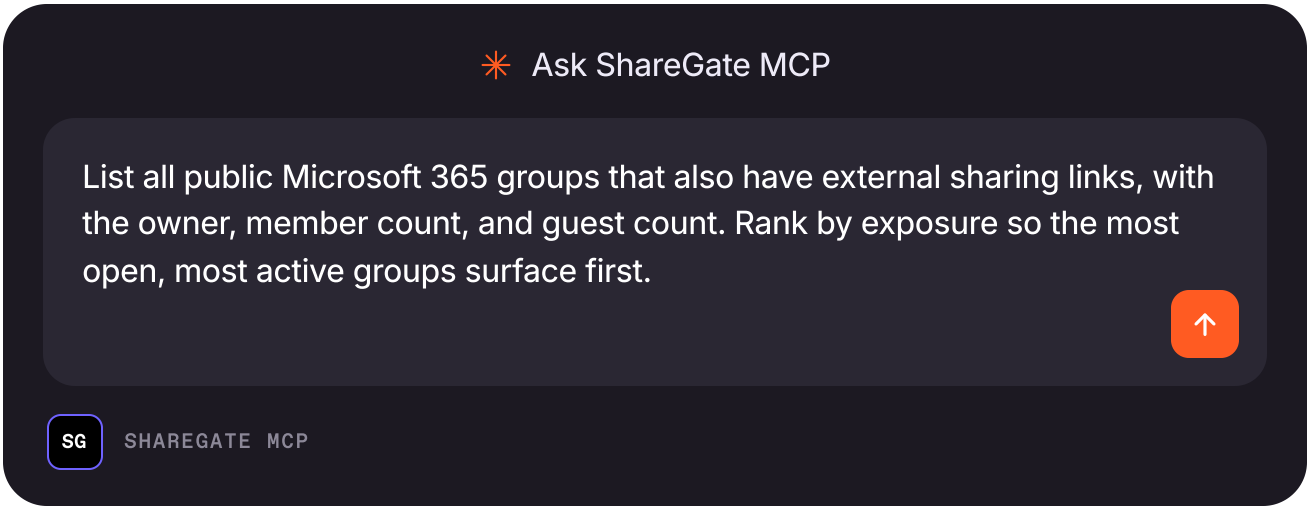
PREVENT OVERSHARING

Public groups with external sharing

USE CASE

You need to find the workspaces that combine two amplifiers—public visibility inside the org and active external sharing—because that combination is where guests see things they shouldn't. Either alone may be fine, but together they mean business content is open internally and reachable by outsiders. Run this prompt to catch the riskiest sprawl pattern in one query ahead of a security review or when tightening collaboration boundaries. It combines two oversharing signals so the genuinely exposed groups rise above the noise of merely-public or merely-shared ones.

THE PROMPT



INSTRUCTIONS

- Write for a non-technical reader. Convey that the group is open to all staff and reachable from outside with one short technical line per entry for admins (group name, visibility, guest count, external link count). Present findings in a single table. Use bullets only for risks and steps.
- Rank highest-to-lowest exposure, top 10 only (note how many remain). If no public groups have external sharing, say so as a positive finding rather than an empty table.

- Score risk on ownership, guest count, and content sensitivity. Public + external + ownerless is the worst combination. Separate plausibly intentional cases (open community, partner space) from accidental drift (an internal project gone open). Don't flag a group on public visibility alone. Flag Copilot exposure where it applies. Public content is broadly surfaceable internally, and external sharing widens it beyond the org. State data currency (last completed crawl, not live status).
- For each finding, give a specific action tied to that group, grouped by urgency: immediate (ownerless or sensitive public + external groups to lock down now), short-term (public groups with external links to review with the owner), ongoing (recurring public-group review + default-private standard for new groups).
- Cite only official Microsoft Learn or ShareGate docs (no invented URLs). If results are extensive, summarize and point to Protect's reports and export for the full CSV. End with one logical follow-up, such as auditing the external links or guests inside the most exposed group.

PARAMETERS · OPTIONAL SWAPS

Visibility focus public groups by default.

`INCLUDE PRIVATE` → *"...also include private groups that have external sharing, flagged separately."*

External type any external sharing by default.

`ANONYMOUS ONLY` → *"...only groups with 'anyone with the link' shares, not just named guests."*

Ownership filter all by default.

`OWNERLESS ONLY` → *"...only public, externally-shared groups that also have no owner."*

06

PREVENT OVERSHARING

Permissions on a target site

USE CASE

A leader or compliance reviewer just asked "who has access to this site?" and you need a clean answer that holds up across IT, the site owner, and whoever's signing off on the access review. This prompt builds a who-can-access-what map for one specific site—every user and group with access, and the level each one holds. Where the other prompts scan broadly, this goes deep on a single high-value target: a finance site, an executive workspace, a client project room. Run this for a least-privilege audit, to answer a "who can see this?" question from leadership or compliance, or to verify access before granting a sensitive site to Copilot. It's the focused drill-down you reach for once a broad sweep has flagged a site worth examining.

THE PROMPT

✳ Ask ShareGate MCP

Build a permissions matrix for [site name]. List every user and group that has access, the access level each holds (owner, member, edit, view), and whether any access is broad (Everyone / All Company / EEEU) or external. Organize it so the broadest and most external access is easy to spot.

SG SHAREGATE MCP

INSTRUCTIONS

- Write for a non-technical reader, with one short technical line per entry for admins (principal name, type, access level, direct vs. inherited). Present findings in a single table. Use bullets only for risks and steps.

- Order access from broadest to narrowest—broad grants and external access at the top, individual view-only at the bottom. Show the full picture, but summarize the long tail with counts if the list is very large. If access is clean and tightly scoped, say so as a positive finding.
- Flag specifically: any broad grant (Everyone, All Company, EEEU), any external or guest access, any group whose own membership is large or externally-capable, and any elevated access (owner/edit) held by someone who looks like they shouldn't have it. Note that group-granted access depends on the group's current membership, which may itself need expanding to see the real reach.
- Be honest about scan state. If the detailed per-principal crawl hasn't finished, say so plainly and point to ShareGate Protect's reports rather than presenting a partial matrix as complete. State data currency (last completed crawl, not live status).
- Note the Copilot exposure angle: the permissions report determines what Copilot can surface from this site. Anyone on this list can have the site's content appear in their Copilot results.
- For each flagged finding, give a specific action tied to that object, grouped by urgency: immediate (external or broad access on a sensitive site to remove or justify now), short-term (elevated individual access to review with the site owner for least privilege), ongoing (a recurring access review and group-membership hygiene).
- Cite only official Microsoft Learn or ShareGate docs (no invented URLs). If results are extensive, summarize and point to Protect's reports and export for the full CSV. End with one logical follow-up, such as expanding the membership of the broadest group on the matrix to see who it really reaches.

PARAMETERS · OPTIONAL SWAPS

Target replace [site name] with the site to audit.

`EXAMPLE` → *"...for the Executive Leadership site."*

`ONEDRIVE` → *"...build the matrix for [user]'s OneDrive instead of a site."*

Access focus all access by default.

`EXCEPTIONS ONLY` → *"...show only broad, external, or elevated access, skip ordinary view-only."*

Group handling list groups as principals by default.

EXPANDED → *"...expand group membership so I see the individual people each group grants access to."*

What's next

These six prompts are just the start. ShareGate MCP turns every type of data Protect tracks into something you can ask for in plain language. And starting in July 2026, something you can act on, too.

Book a demo → to walk through how it works with one of our experts, or start a **free Protect trial**. ShareGate MCP is included.

Already a ShareGate Protect customer? **Connect ShareGate MCP today →** it's included in your plan.

ShareGate