FREE ADMIN RUNBOOK · COPILOT READINESS

The EEEU cleanup runbook

Find every file, folder and site shared with Everyone or Everyone except external users, before Copilot does.

PAGE 1 OF 2 · RUN THE REPORT

Matt Berry Tech
Oct 2026 · v1.1

READ FIRST **Global Admin can't run this report.** It needs the **SharePoint Advanced Management Administrator** role, and a Global Admin has to assign it, even to themselves. That's by design: it's the role that can see file names and paths across every site.

01 Before you start

- [ ] **SAM Administrator role** assigned and active.
  `Entra admin center > Roles & admins`
- [ ] **SharePoint Advanced Management** available. One assigned Microsoft 365 Copilot license turns it on; otherwise you need the SAM Plan 1 add-on.
- [ ] **Baseline report run once:** "Site permissions across your organization." The first run can take up to 5 days, so start it early.

02 Run it

1. **Run the baseline** if it has never run. Include SharePoint and OneDrive.
   `SharePoint admin center > Reports > Data access governance > Site permissions across your organization`
2. **Assign the role.** Search "SharePoint Advanced Management Administrator" > Add assignments > add yourself or your governance admin.
   `Entra admin center > Roles & admins`
3. **Confirm it's active.** Your account's assigned roles should list it as "Direct." Using PIM? Activate it first.
4. **Sign out and back in.** The open session keeps the "you need a role" banner until you do. An InPrivate window is a quick test.
5. **Run both reports:** Everyone, and Everyone except external users. Each has its own tile.
   `Data access governance > Snapshot reports > Sites and files shared via special SharePoint groups > View reports > Run report`
6. **Download** when the status says "Report available." You get a ZIP with a CSV inside. Expect hours: start it at the end of the day.

03 The four snags

No Run report button
You're missing the SAM Administrator role. Global Admin isn't enough.

The role banner won't go away
New role, old session. Sign out and back in.

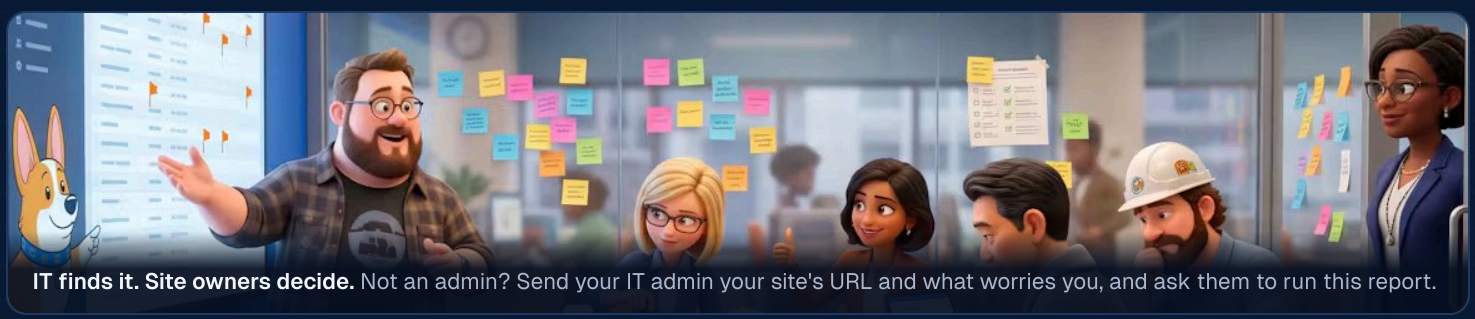
The report won't generate
The baseline "Site permissions" report hasn't run yet.

You can only run it every 30 days
Don't spend a rerun checking yesterday's fixes. Use the site's own permissions page for that.

04 Timing at a glance

5 days max first run of the baseline report	**Hours** item-level report, in our test
48 hrs how old the data can be	**30 days** between reruns
1M rows cap on the CSV download	**~15 min** hands-on time, no PowerShell

Report downloaded? Turn to page 2: how to read the CSV, the exact clicks to fix it, and how to bring site owners in.



IT finds it. Site owners decide. Not an admin? Send your IT admin your site's URL and what worries you, and ask them to run this report.

Sources: Microsoft Learn (Data access governance reports, item-level EEEU report, SAM prerequisites) · Message Center MC1450131



Fix what you find

Read the CSV by pattern, close the big exposures, and hand site owners a list they can act on.

Matt Berry Tech
Oct 2026 · v1.1

05 Read the CSV by pattern

YOU SEE	IT MEANS	PRIORITY
`ItemType = Web` + `ParentGroupType` = SharePoint group	EEEU is in a site's Members or Visitors group. The whole site is open.	Fix first
`File` / `Folder`, no parent group	One item shared directly with the group.	Owner cleanup
`LinkId` / `LinkScope` filled in	Access comes through a sharing link.	Review link
High `TotalUserCount`	Many people open it. Biggest exposure, easiest to break.	Go gently

Pivot on **SiteId** for one list per site. Big file? Load it with Power Query. Skip system groups such as Style Resource Readers. Run both CSVs: "Everyone" rows can include guests, so look at those first.

Don't stop at EEEU. "People in your organization" sharing links open files org-wide too, and this report doesn't count them. Run **Data access governance > Sharing links > People in your organization** as well.

06 The exact clicks

Whole site open (EEEU in a site group)

`Site ⚙ > Site permissions > Advanced permissions settings > open the Members or Visitors group > tick Everyone except external users > Actions > Remove Users from Group`

Single file or folder

`Select the item > Manage access > Groups tab > select the group > Remove access`

Public Team or Microsoft 365 group

`A public group puts EEEU in its site's Members group. Making it private removes it, but also changes who can find and join the Team. Ask the owner first.`

07 Send a site access review

1. **Open a supported report:** "Shared with 'Everyone except external users'" (activity) or "Site permissions across your organization."
   `Reports > Data access governance > View reports`
2. **Select the sites**, up to 100 at a time, then **Initiate site access review**.
3. **Customize and preview email** with a short "why," then **Send**.
4. **Track it** on the **My review requests** tab. Owners mark the review complete and their comments come back to you. Limit: 1,000 a month.

08 Work it with site owners

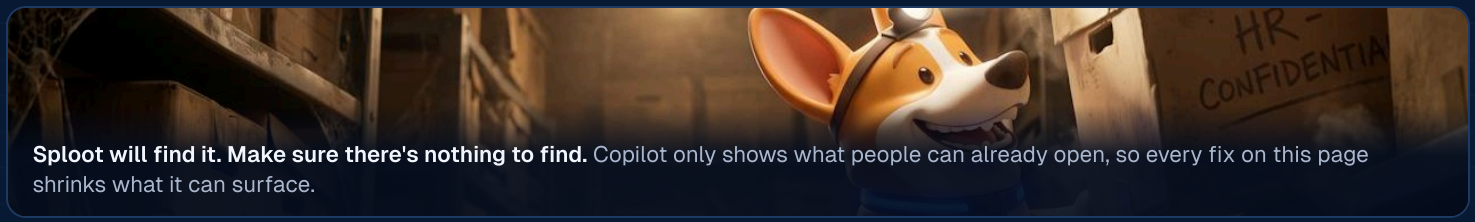
1. **Close the obvious ones yourself,** so you can say "we've already fixed these."
2. **Give each owner only their own list,** sorted by TotalUserCount. No blanket emails.
3. **Three choices per item:** keep org-wide on purpose, narrow to a group, or remove.
4. **Rerun every 30 days** and track the count. That's your governance number.

IT	Site owners	Creators	Leadership
Owns the process and the report	Decide about their content	Explain what they meant	Watches the trend

09 Stop new exposure & PowerShell

```
# Connect (SPO Management Shell 16.0.27215.12000+, no -Credential)
Connect-SPOService -Url https://<tenant>-admin.sharepoint.com
# Hide EEEU from the people picker (existing grants stay)
Set-SPOTenant -ShowEveryoneExceptExternalUsersClaim $false
# Run the report (or -ReportEntity Everyone), check, export
Start-SPODataAccessGovernanceInsight -ReportType Snapshot `
  -ReportEntity EveryoneExceptExternalUsers
Get-SPODataAccessGovernanceInsight
Export-SPODataAccessGovernanceInsight -ReportID <id> `
  -DownloadPath <folder>
```

Needs the SAM Administrator role. While you clean up, **Restricted Content Discovery** keeps a sensitive site out of Copilot and search. Treat the SAM Admin role as privileged: named people, PIM-eligible, time-limited.



Sploot will find it. Make sure there's nothing to find. Copilot only shows what people can already open, so every fix on this page shrinks what it can surface.

Sources: Microsoft Learn (Site access reviews, DAG PowerShell, item-level EEEU report, EEEU and private groups) · page 1 steps tested in a production tenant, Oct 2026; page 2 from Microsoft docs