THE "OVERSHARED" POLICY

An internal audience that is too wide

Overshared puts in front of each object's owner the internal audience the vendor makes verifiable: access open to the whole organisation, groups deemed too broad, the number of organisation links, the number of people. That audience is compared with the thresholds you set. The owner confirms the audience or narrows it, and the decision is recorded.

VERSION
1.0 · October 2026

READERS
Access governance lead, workspace administrator, reviewer

DISTRIBUTION
Confidential · REVIEWIT customers

IN THIS SHEET

01 The problem: access nobody decided
02 A question of its own
03 The philosophy: five commitments
04 The four signals and the settings that answer them
05 How the audience is counted
06 Resource by resource
07 The verdict
08 What the reviewer does
09 What the policy does not do
10 Running a campaign
11 Glossary

THE FOUR SIGNALS AT A GLANCE

ORGWIDEACCESS	AUDIENCEGROUPS	ORGLINKCOUNT	AUDIENCESIZE
Organisation-wide access	**Audience groups**	**Organisation links**	**Audience size**
A grant to the whole organisation, with role and path.	The directory groups that grant access, named.	"People in your organisation" links, dated by the report.	A proven floor, with its completeness indicator.

01 The problem: access nobody decided

A team site is created for twelve people. Three years later it carries forty "people in your organisation" links on its files, an "All employees" group was added to the members to unblock a project, and nobody remembers. Nothing has left the company, no guest has come in, the site is still declared "private". And yet its contents are within reach of five thousand people.

That is oversharing: the gap between an object's intended audience and the audience that can actually reach it. It settles in through small, legitimate gestures, it triggers no alert, and it stays invisible until a search tool or an assistant makes findable what was merely accessible. Enterprise assistants create no access: they reveal the access that already exists.

02 A question of its own

REVIEWIT asks each policy a single question, readable in a verifiable fact. Overshared duplicates none of its neighbouring policies:

POLICY	THE QUESTION	THE FACT READ	BOUNDARY
Privacy	Is the declared visibility the intended one?	An object setting: public or private	What the object announces
External Sharing	Is sharing outside the organisation justified?	The external sharing level, "anyone" links	The organisation's boundary
Guests	Does each guest still have a reason for access?	Named external people	One external person
Membership, Permissions	Should each holder stay, at this level?	A nominative access	One person, one at a time
Overshared	Who, inside the organisation, can actually reach the object, and is that wider than its use?	An organisation-wide grant, organisation links, a counted audience	The effective internal audience, taken as a whole

A "private" object can be open to everyone: Privacy calls it compliant, Overshared sees it. A nominative review does not see the "everyone" claim, which is not a person: Overshared reads it. When the vendor's visibility setting itself means "the whole organisation" (a workspace-public project, an internal repository, a public channel), Privacy judges it and Overshared does not judge it again: Overshared only retains grants and measured audiences.

03 The philosophy: five commitments

01 **Measure what can be verified, never assume.**

Every signal comes from a source the vendor documents: a member list, a member count, an administration report. A signal the vendor does not provide is not written, and the corresponding criterion is not evaluated. *Absent is never zero.*

02 **A verifiable minimum, and say whether it is complete.**

The number of people in an audience is always a proven floor, with a completeness indicator. When a group could not be expanded, or access is open to the whole organisation, the number stays a minimum and the object says so. A minimum above the threshold is a fact; an incomplete minimum below the threshold is not compliance.

03 **The threshold belongs to the organisation.**

"Too many" depends on use: three hundred people for an executive site, three thousand for a division's intranet. REVIEWIT sets no default numeric threshold; it only rules on the binary fact, organisation-wide access, and leaves the numbers to the customer.

04 **The verdict says what the audience is; the decision stays with the owner.**

A wide audience can be intended: intranet, communication site, company-wide community. The reviewer confirms with a reason, requests a reduction or escalates. Every decision is recorded and defensible.

05 **Aggregates, never content.**

The signals are grant text and numbers. REVIEWIT reads no file, no message, does not judge the sensitivity of content and does not keep the item-by-item detail of an administration report. The sensitivity label is known only by its identifier.

04 The four signals and the settings that answer them

SIGNAL CARRIED BY THE OBJECT	MEANING	CAMPAIGN SETTING	DEVIATION IF
Organisation-wide access `OrgWideAccess`	Grants to the entire organisation, in the vendor's words, with role and path: "Everyone except external users · Edit · via Site members"	Allow organisation-wide access (yes/no, no by default)	A grant is present and not allowed
Audience groups `AudienceGroups`	The directory groups that grant access, named	Groups deemed too broad, picked from your directory ("All employees", a dynamic group)	One of the chosen groups grants access
Organisation links `OrgLinkCount`	The number of active "people in your organisation" links, as counted by an administration report, with its as-of date	Maximum number of organisation links	The number exceeds the maximum
Audience size `AudienceSize` · **completeness**	The number of people who can reach the object, proven floor	Maximum audience	The number exceeds the maximum, even if the count is incomplete

DEVIATION MODE

One last setting says what a deviation does to the overall verdict: in **strict** mode, one criterion in deviation makes the object non-compliant; in **lenient** mode, each deviation stays visible criterion by criterion and the overall verdict remains compliant. Lenient mode serves a first observation campaign.

05 How the audience is counted

This is the most frequent question: **who computes the audience, and do nested groups count?** Nobody computes the threshold: it is your setting. The audience is measured by collection, at pass time, with the same rules for every resource:

- A **named person** counts once, by their resolved identity. An identity the vendor does not allow to resolve makes the audience incomplete.

- A **directory group** is named, then counted by the number of users it reaches by traversing its sub-groups down to people. Nested groups are therefore taken into account. Because members of several groups overlap, their sum would prove nothing: REVIEWIT keeps the largest count and marks the audience incomplete. A group that cannot be counted stays named; nothing is invented.
- **Organisation-wide access** is reported, never counted. It makes the audience incomplete: the number of people is then "at least N".
- **Organisation links** cannot be read through programming interfaces: they come from the vendor's administration report, which you import into REVIEWIT as a supplementary import. Each value carries the report's as-of date, shown with the criterion, and stops being taken into account after sixty days.

The audience is thus read at the level of the collected object: the site, the team, the community, the workspace. File-by-file detail is not covered; the administration report aggregates it per object, which is what the supplementary import brings.

06 Resource by resource

RESOURCE	WHAT IS MEASURED	NESTED GROUPS	COMPLETE AUDIENCE?
SharePoint site	People from the site's grants, granted groups named and counted, organisation-wide access; organisation links through the import of the site permissions report	Yes, by transitive group count	No as soon as a group or organisation-wide access is present
OneDrive	Organisation links and the number of users with access, through the import of the same report	Not applicable	Per the report
Teams team	People from the team's member list (owners, members, guests)	Not applicable: a team's members are people, a Microsoft 365 group contains no group	Yes, if every member is named
Viva Engage community	Members of the linked Microsoft 365 group	Not applicable, same reason	Yes; a community open to the whole network without a member list has no audience and is not evaluated
Power BI workspace · coming	Links shared with the whole organisation, granted groups named	Not expanded at first	No
Exchange public folders, shared mailboxes · coming	After proof of the meaning of "default" access	To be specified	To be specified
Cloud resources	Access open to the customer's whole organisation (bucket policy, organisation sharing), when the vendor makes it verifiable	Not applicable	Not applicable

A Teams team and its SharePoint site are two objects: a security group added by hand in the site is read on the site, not on the team. Each is evaluated with its own audience.

07 The verdict

CRITERION	EXPECTED	OBSERVED
Organisation-wide access	"No organisation-wide access" or "allowed for this campaign"	The grant text, or "none"
Groups deemed too broad	"None of the chosen groups"	The groups found
Organisation links	"At most N links", with the report's as-of date	The number
Audience size	"At most N people"	"N people" if the audience is complete, "at least N people" otherwise

THREE READING RULES

01

Out of scope, stated as such

An object carrying none of the four signals has no Overshared verdict: the sheet shows it without judging, it never displays compliance by default.

02

A floor above the threshold is a deviation

Even incomplete, an audience of "at least 40 people" exceeds a threshold of 30.

03

An incomplete floor below the threshold is not evaluated

"At least 12 people" against a threshold of 30 proves nothing: the criterion is left open rather than asserting compliance.

08 What the reviewer does

The reviewer is, in principle, the object's owner: they know the use, they often opened the access themselves. They see the grant, the path, the groups, the numbers and their dates. They have three gestures:

Confirm the audience

With a reason: intranet, communication site, company community. The reason is kept and resurfaces at the next campaign.

Request a reduction

Remove the grant, convert the links, take a group out. The reduction is a write gesture at the vendor, followed up by remediation.

Escalate

Through the review's usual mechanisms.

They are not asked to judge the sensitivity of content they do not see in REVIEWIT, nor to change tenant settings: that is the vendor administrator's business.

09 What the policy does not do

- It does not eliminate oversharing: it makes it visible, measured and decided.
- It certifies no readiness for an enterprise assistant: it helps with it.
- It does not detect sensitive content and reads no content.
- It does not cover an object's item-by-item detail; it reads the object, and the administration report that aggregates it.
- It changes nothing at the vendor: narrowing an audience is a decision, then a remediation.

10 Running a campaign

01 **Choose the workspace and the resource**
Overshared is offered to workloads carrying at least one of the four signals: today SharePoint, OneDrive, Teams and Viva Engage.

02 **Import the administration report**
If the campaign covers organisation links (sites, OneDrive): Subscription Manager › Collect › Import a report, format "Supplementary import". See the sheet "The supplementary import".

03 **Set the policy in the Overshared panel**
Organisation-wide access allowed or not, the groups deemed too broad picked from the directory, the maximum number of links, the maximum audience, the deviation mode. Numbers left empty are not evaluated.

04 **Designate the reviewers**
The object's owners, with a fallback reviewer for objects without an owner.

05 **Read the results criterion by criterion**
Then let the reviewers confirm or narrow. A first campaign in lenient mode lets you observe the distribution of audiences before setting the thresholds of a strict campaign.

EXAMPLE

Fifty-six Teams teams, all counted with a complete audience, from two to eighteen people. A maximum audience of fifteen surfaces six public teams: the running club, the after-work group, the social committee, the Power Platform community, the newcomers and the company-wide team. Their owners confirm the first five as intended communities and the sixth as the company team; the campaign has established, and recorded, that these audiences are owned.

11 Glossary

Internal audience	All the people in the organisation who can reach an object, through direct access, a group or a link.
Organisation-wide access	A grant whose beneficiary is the entire organisation ("Everyone except external users", "All"), whatever the path.
Organisation link	A sharing link anyone in the organisation can open.
Proven floor	The number of people REVIEWIT was able to name or count; the real audience is at least that.
Supplementary import	Adding, to objects already collected, the columns only an administration report knows, with its as-of date.
Deviation mode	Strict, a deviation makes the object non-compliant; lenient, deviations are visible and the overall verdict rem ains compliant.

This sheet describes the policy as REVIEWIT implements it at publication date. The signals read depend on what each vendor makes verifiable; they may evolve with later versions.