

SHARING · COLLABORATION · GOVERNANCE

Share the work. *Not the workspace.*

Most platforms make sharing binary: invite someone into everything, or email them a copy that starts going stale immediately. portablemind shares the work itself — a project, a conversation, a file, a board, even an AI agent — with a person, a team, or another company entirely, at exactly the level you choose. And underneath, every grant is a first-class security object with provenance, an optional expiry, and an audit trail.

9

KINDS OF WORK,
ONE SHARE VERB

5

PERMISSION
LEVELS, VIEWER TO
OWNER

Cross-org

DIRECTED SHARING
BETWEEN COMPANIES

THE ALL-OR-NOTHING TRAP

Collaboration shouldn't cost you the building.

The moment work crosses a boundary — a contractor, a client, a partner company — most tools give you two bad options and call it collaboration.

01

The over-invite

To show a client one project, you add them to the whole tool — and hope nobody notices what else they can see.

02

The stale copy

Export it, email it. Now there are two versions, no way to revoke, and no idea who has it six months later.

03

The per-app maze

Documents share one way, tasks another, chat not at all. Every silo has its own rules — and its own leaks.

04

The unaccountable grant

Someone has access. Who gave it to them? When? Why? Most tools can't answer — so nobody dares clean up.

Every grant knows why it exists.

When someone can see a piece of work in portablemind, the system doesn't just know *that* — it knows *why*. Six distinct share types are tracked on every grant, so audits mean something and revocation is safe: remove the reason, and the access that rode on it goes too.

01 Owner

The creator's party or owning team. Full control from the moment the work is born.

02 Direct

Explicitly granted to a person, by name, at a chosen level.

03 Team

Granted to a team — access follows membership, so joining and leaving update it automatically.

04 Cascaded

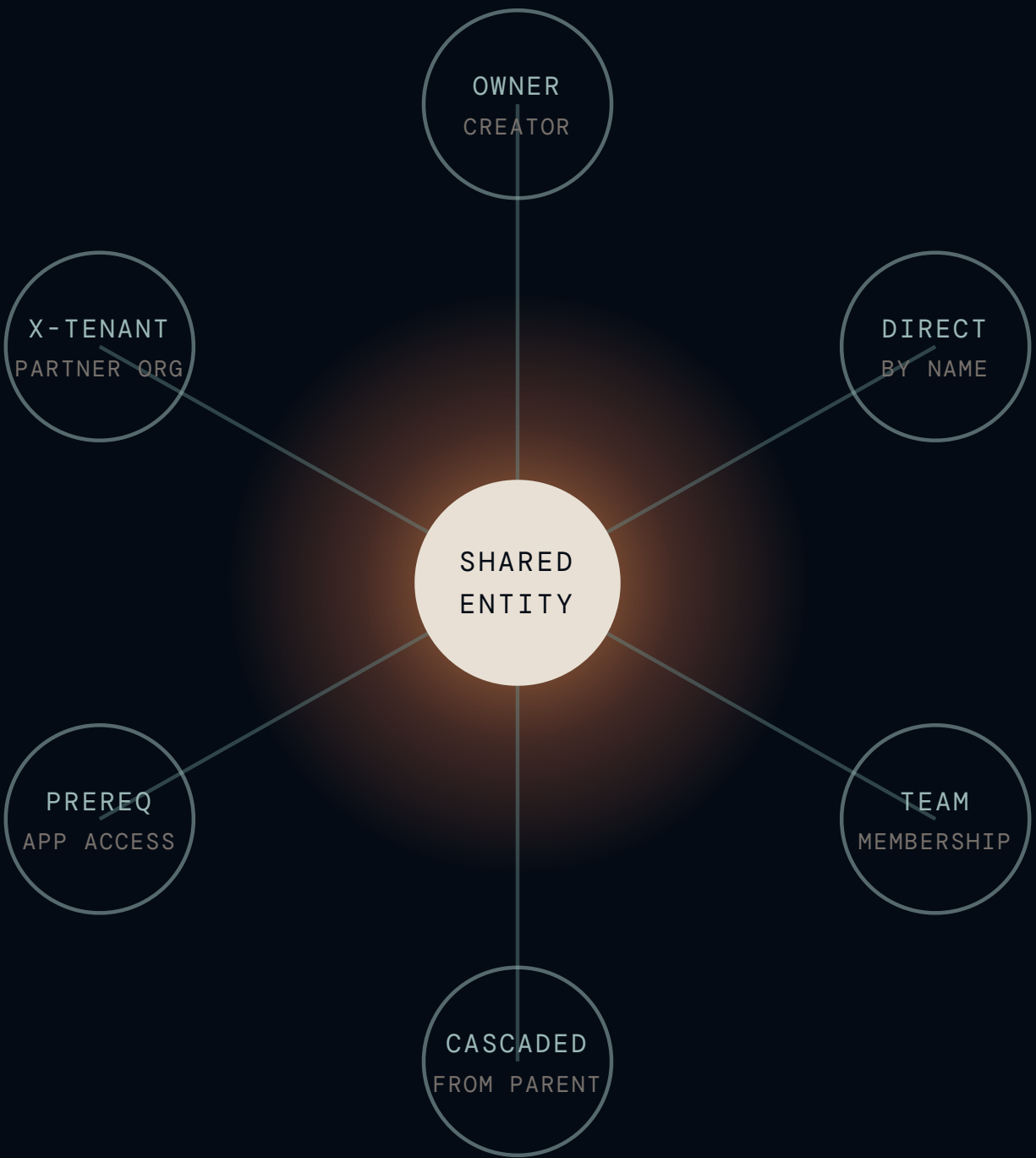
Inherited from a parent: tasks from their project, attachments from their conversation.

05 Prerequisite

Auto-granted app access, so a share arrives usable instead of locked behind a missing module.

06 Cross-tenant

Granted from another company — without either side giving up its isolation.



ONE VERB, NINE KINDS OF WORK

If your team makes it,
your team can share it.

Sharing isn't a feature of one app — it's platform infrastructure. Nine entity types share through the same machinery, with the same permission levels, the same audit trail, and the same revocation story.

WORK

Projects

Share a project and its tasks come along — including tasks created after the share.

WORK

Tasks

Shareable on their own, or inherited automatically from the project they belong to.

WORK

Kanban boards

Hand a partner the board view of the work, at whatever level you choose.

KNOWLEDGE

Conversations

Share a team chat and its attached files ride along, so context arrives whole.

KNOWLEDGE

Files

One live document instead of emailed copies — revocable, expirable, audited.

KNOWLEDGE

Folders

Share a folder and its contents inherit access — while private files inside stay private.

OPERATIONS

Tickets

The unit of cross-company support: share tickets to a provider, with their chats and files in tow.

OPERATIONS

Saved views

Share the exact filtered lens on the work, not just instructions for rebuilding it.

INTELLIGENCE

AI agents

A configured AI teammate is shareable like a document — hand a colleague the agent, not a setup guide.

ACCESS LEVELS

Five rungs between "can peek" and "can delete."

LVL 1	Viewer	Read-only. Sees the work, touches nothing.
LVL 2	Commenter	Views and comments — feedback without the ability to alter the thing itself.
LVL 3	Editor	Changes the content, not the audience — and can't delete what someone else owns.
LVL 4	Full Access	Edits, re-shares, and can delete. Everything but ownership itself.
LVL 5	Owner	The entity's anchor: full control, and the identity every other grant traces back to.

When multiple shares apply, the highest level wins — a viewer grant from a team and an editor grant by name resolve to editor. Any share can carry an **expiration date**; expired grants are swept nightly and the expiry is logged like any other access change.

THE GRANTEE SPECTRUM

From the desk next to you to a company you've never onboarded.

Grantee 01

A person

The Google-Drive move: pick a person, pick a level, done. The grant is **individually revocable**, optionally expiring, and recorded with who gave it and when.

BY NAME

ANY OF 5 LEVELS

OPTIONAL EXPIRY

Grantee 02

A team

Teams are first-class citizens, not mailing lists. Share to a team and **access follows membership**: new members see the work the moment they join, departing members lose it the moment they leave — no share cleanup required. Teams themselves can be open, closed, or hidden.

MEMBERSHIP-DRIVEN

OPEN / CLOSED / HIDDEN TEAMS

ZERO CLEANUP

Grantee 03

An email that isn't a user yet

Share to any email address. If it's not on the platform, a **pending invitation** goes out with a secure, time-limited token — and the share activates the moment they create their account. They get **their own workspace**, not a squatter login inside yours; if they already have an account at another company, the systems link up automatically.

INVITE BY EMAIL

TIME-LIMITED TOKEN

ACTIVATES ON SIGNUP

Grantee 04

Another company

Directed cross-organization sharing is where most platforms simply stop. Here, sharing with someone at a partner company **establishes a governed relationship between the two organizations** — automatically, on the first share. The data never moves: the grant lives in the owner's tenant, the partner sees exactly the entities shared with them, and **tenant isolation holds on both sides**. Relationships can be suspended, reactivated, or revoked — and revocation pulls the access that rode on them.

For ongoing partnerships, ticket sharing can run in **auto mode** — every new ticket flows to the provider — or ticket-by-ticket. Internal AI conversations are **structurally excluded**: an AI chat can never be shared across the company line.

DATA NEVER COPIED

SUSPEND / REACTIVATE / REVOKE

AUTO OR PER-TICKET

AI CHATS STAY HOME

STRUCTURE-AWARE

Sharing follows the shape of the work.

Real work isn't flat. Projects contain tasks, conversations carry files, folders nest. A share that stops at the surface is a share that breaks the first time someone opens an attachment.

Behavior 01

Access cascades down

Share a project and its tasks come with it. Share a conversation and its attached files arrive too. Share a folder and the tree inherits. And it stays true over time: **work added to a shared parent later inherits the parent's shares automatically** — no "why can't the client see the new task" tickets.

PROJECT → TASKS

CHAT → ATTACHMENTS

FOLDER → CONTENTS

LATE ADDITIONS INCLUDED

Behavior 02

Private stays private

Inheritance never overrides privacy. A **private file inside a shared folder stays hidden** until its owner shares it directly. Cascades widen access along the paths you chose — they don't flood the basement.

PRIVACY WINS

DIRECT SHARE TO OVERRIDE

Behavior 03

Revocation with eyes open

Taking access away is as structured as granting it. Revoke a share and its cascaded grants go with it. And when a revocation would be undermined by access still flowing from a parent, the system **tells you what else is involved before acting** — no silent lockouts, and no false confidence that access is gone when it isn't.

CASCADE-AWARE REVOKE

DEPENDENCY PROMPT

BULK REVOKE PER GRANTEE

Every share is a security object, not a checkbox.

Sharing isn't bolted onto the platform — it's built out of the same capability engine that runs role-based access control. That one design decision is where most of the guarantees below come from.

Audited end to end

Every grant, level change, revocation, and expiry is logged: who shared what, with whom, at what level, and whether it arrived by cascade or from another company.

Enforced twice

Lists are filtered in the database before results exist, and every write is re-checked against the grantee's per-entity level. A broad role never quietly overrides a narrow share.

Expiring by design

Contractor ends in 30 days? Set the share to expire with the contract. A nightly sweep removes expired grants and writes the expiry to the audit trail.

Arrives usable

Sharing a file with someone who's never used the Files app auto-grants the prerequisite app access — a share opens on the first click instead of a permissions error.

Agents share alike

AI agents act through real, governed identities. An agent sees exactly what its identity has been granted — owner, team, cascaded, or cross-company — with no privileged bypass.

Flat-cost at scale

Share lookups run on dedicated indexes, so a user with hundreds of shares queries as fast as a user with three. Cross-company visibility resolves in a fixed handful of queries regardless of partner count.

WHERE WE'RE HONEST

Every share on the platform today is granted to an **identity we can audit** — a person, a team, a partner organization — never to "anyone with the link." Anonymous public links for entities are on our roadmap, and they'll ship only when they meet the same provenance and revocation bar as everything above. If a control isn't real yet, we won't put it on a slide. That discipline is exactly why you can trust the ones that are.

Share one project. Not the building.

See how directed sharing works between real organizations — and what it would take to run your client and partner collaboration on it.

TALK TO US ABOUT SHARING

↓ [DOWNLOAD THIS BRIEF \(PDF\)](#)