WHITE PAPER

External Sharing & Guests.

Open for a project. Open forever?

Why sharing with outsiders outlives its purpose, and how to certify external sharing and guest access before they become a standing exposure.

EXECUTIVE SUMMARY

Sharing is opened in a minute. It is rarely closed again.

Collaboration platforms make it trivial to share a space, a folder or a channel with a partner, a supplier or a consultant. That is their value. The problem is time: sharing is granted for a project, and stays when the project ends.

Guest accounts follow the same pattern. Invited for a few weeks, they remain for years, often with no internal sponsor left to answer for them.

This paper describes how to certify external exposure from two sides: the resource that is shared, and the guest who has access, with decisions that are explicit, owned and time-bound.

Two sides
The shared resource, and the guest who reaches it.

A named sponsor
Every guest has someone inside who answers for them.

Time-bound by design
Exceptions carry a reason and an end date.

Verified closure
A closed share is confirmed by a later observation.

CONTENTS

01 How exposure accumulates
02 The resource side
03 The guest side
04 What regulators expect
05 Closing what was opened
06 Where to start

01

How exposure accumulates

External sharing rarely starts as a risk. A team opens a space to a partner to work faster; a manager invites a consultant; a link is sent to a supplier. Each decision is reasonable on the day it is taken.

What makes it a risk is that nobody is asked again. The project ends, the partner changes, the consultant leaves, and the access remains. Over a few years, the organisation accumulates an external audience it can no longer describe.

“Sharing granted for an assignment is rarely closed again.”

KEY IDEA

DEFINITION

External exposure: the set of resources reachable by people outside the organisation, through sharing, links or guest accounts.

02

The resource side

From the resource's point of view, the question is not who each guest is, but whether the resource should be open to outsiders at all, and to which audience.

An external sharing policy puts that question to the owner of the resource. The decision is to confirm the sharing, restrict it, or close it. Two related policies complete the picture: privacy, which compares the visibility of the resource with the level intended for its content, and internal oversharing, which looks at audiences that are too wide inside the organisation.

"Is sharing it outside the organisation still justified?"

KEY IDEA

- **External sharing.** Is sharing outside the organisation still justified?
- **Privacy.** Does the visibility level match the intended level?
- **Internal oversharing.** Is the internal audience wider than it needs to be?

03

The guest side

Guest accounts deserve a policy of their own. The first question is not technical: who invited this person, and who answers for them today? A guest without an internal sponsor is an access without an owner.

The review asks the sponsor whether the guest still needs access, to what, and until when. Where an exception is granted, it carries a reason and an end date, so that it expires unless someone renews it.

“Every guest needs someone inside who answers for them.”

KEY IDEA

Sponsor
A named person inside the organisation.

Scope
The resources the guest actually needs.

Duration
An end date, not an open-ended invitation.

Renewal
A new decision, not a silent extension.

04

What regulators expect

Third-party access is a recurring theme of security frameworks. NIS2's implementing regulation asks that third-party access be limited in scope and duration; DORA's technical standards extend access control to the staff of ICT third-party service providers; ISO 27001 and SOC 2 expect access to be removed when no longer authorised.

A certification that covers external sharing and guests, with sponsors, end dates and verified closures, answers those expectations with records rather than intentions.

“Third-party access, limited in scope and duration.”

KEY IDEA

05

Closing what was opened

A decision to close a share or remove a guest is a beginning, not an end. The correction is tracked until a later observation confirms that the share is closed or the account removed.

The evidence then tells a complete story: the exposure observed, the owner or sponsor who decided, the date, the reason, and the confirmation that the change took effect.

“A closure counts only when it is observed.”

KEY IDEA

DEFINITION

Verified closure: a share or guest access considered removed only once a subsequent collection shows it is gone.

06

Where to start

External exposure is best reduced step by step, starting where the stakes are highest.

"Start where the most sensitive content is shared the widest."

KEY IDEA

1 **Map external sharing** on the platforms that hold sensitive content.

2 **Name a sponsor** for every guest account.

3 **Certify shares with their owners** and guests with their sponsors.

4 **Make exceptions temporary,** with a reason and an end date.

5 **Verify every closure** and keep the evidence.

REVYCORE

Open when needed, closed when done.

Human decisions. Verifiable evidence.

Request a demonstration in your context: your solutions, your scopes, your agents.

revycore.com

This paper describes an approach and the corresponding capabilities of REVYCORE for information purposes; it is not legal advice. The policies that apply depend on the nature of each resource and on what each solution allows to be observed. © 2026 REVYCORE SAS.