



MAINTAINING CONTROL OVER SHARED PROJECT FILES

How one organization protected sensitive documents across distributed collaboration workflows without disrupting how teams work.

Situation

A project-driven organization regularly shares RFPs, contracts, pricing documents, and project materials with vendors, external collaborations, and affiliated stakeholders.

As files moved between shared drives, endpoints, email, and external recipients, maintaining consistent visibility and control became increasingly difficult.

The Governance Gap

Existing controls helped secure repositories, shared drives, and collaboration platforms, but governance often stopped once files were downloaded, copied, emailed, or retained externally.

The organization needed protection that remained with the file itself through out its entire lifecycle.

Challenge

The organization relied heavily on external collaboration throughout project lifecycles, with sensitive files routinely shared across multiple internal and external parties.

As projects evolved, access needs frequently changed, but files often remained downloaded, forwarded, or retained outside the organization's direct control.

- ✓ Sensitive documents shared across multiple external stakeholders.
- ✓ Access requirements changed throughout projects and engagements.
- ✓ Files retained locally after projects ended or roles changed.
- ✓ Limited visibility into how files were accessed or redistributed.
- ✓ Reliance on users to manually apply protections consistently.

Solution

The organization implemented SafeSuite with Intelligent Directory™ to automatically protect sensitive files stored within designated collaboration folders.

As files were added to these folders, embedded protection policies were applied automatically, allowing teams to continue using familiar workflows while maintaining centralized control and visibility.

How It Worked



Sensitive files added to designated collaboration folders.

Intelligent Directory™ automatically applies protection policies.

Files shared through normal workflows.

Policies remain enforced after downloading.

Access updated or revoked as project evolves.

Outcomes



Reduced Governance Burden

Protection policies were applied automatically without disrupting collaboration.



Improved Visibility & Auditability

Teams gained insight into file access activity across distributed collaboration workflows.



Maintained Control After Sending

Access remained enforceable even after files were downloaded, forwarded, or retained externally.



Reduced Risk from Lingering Access

Access could be updated or revoked as projects, vendors, or stakeholder relationships changed.

See how SafeSuite helps organizations maintain control after sharing.
Contact info@keyavi.com for more information.