

Document Management — Least-Privilege by Default

System of record for files: guarded uploads, verification, expiry, and retention.

The document service is the platform's system of record for files — pay documents, HR forms, signed agreements, I-9 evidence, and compliance artifacts — built defensively because document access is a constant audit target. A W-2 or an I-9 is only ever visible to someone entitled to see it, and the read path fails closed.

1 Store, request, verify, retire

Capability	Detail
Least-privilege reads	Every read is authorized by role and tenant — an employee sees their own documents, an admin sees the client's, nothing crosses a tenant boundary, and the path fails closed.
Guarded uploads	Content-type and extension allowlists on upload; a typed document catalog; a document-request workflow so the platform can ask a client or employee for a specific file and track it to receipt.
Verification	Documents can be marked verified, with a state-forms library keyed by state so the right jurisdiction's form is always on hand.
Compliance tracking	Expiring-document tracking with a summary and an expiring sweep (e.g. work authorizations, certifications) so nothing lapses silently.
Retention	A retention policy with a scheduled purge sweep — documents don't linger past their required life, and deletes are real.
Owned, not licensed In-house e-signature — agreements are signed inside the platform, with no third-party e-sign vendor to license and mark up. - Fast delivery even for large files; the same strict, closed-by-default tenant isolation the rest of the platform uses protects every document.	