

Data Retention and Disposal Policy

Effective Date: July 27, 2026

Document Owner: Justin Plane, Chief Executive Officer & CISO

1. Purpose and Scope

This policy outlines the classification, handling, retention, and disposal of data stored, processed, and transmitted by FirmSpan LLC. As a Data Processor acting on behalf of law firms (the Data Controllers), FirmSpan adheres to the principle of data minimization, ensuring that client legal documents, consumer financial data, and system logs are retained only as long as necessary to deliver the service and are securely destroyed when no longer required.

2. FirmSpan's Role: Collection Platform, Not System of Record

This section governs the interpretation of every retention period in this policy and should be read first.

- **Purpose-Built for Intake, Not Archival:** FirmSpan is a document and financial data collection platform. It exists to gather materials from a law firm's clients during an active matter and make them available to the firm. FirmSpan is expressly **not** a document management system, a system of record, a client file archive, or a long-term retention service, and it is not designed, priced, or represented as one.
- **The Firm Remains Custodian of the Client File:** The law firm retains sole responsibility for maintaining the client file in accordance with its own professional, ethical, and jurisdictional obligations, including rules governing safekeeping of client property and return of client files. Those obligations frequently require retention for a period of years and are not discharged, satisfied, or assumed by FirmSpan's retention of a copy.
- **Export Is the Firm's Responsibility:** Customers are responsible for exporting materials from FirmSpan and storing them in their own document management system before the retention periods in Section 4 expire. FirmSpan provides the export capability described in Section 5; the decision to use it, and its timing, rests with the customer.
- **Retention Periods Are Determinate:** Every deletion date under this policy is calculable in advance from the schedule in Section 4. A firm can determine, at the moment a matter is created or archived, the date on which its data will be deleted.
- **Deletion Is a Security Feature and Is Irreversible:** Short retention limits the exposure window for highly sensitive family law and consumer financial data. Once a retention period expires, the data is deleted and FirmSpan cannot recover it.

3. Data Classification and Handling

Classification determines handling. Where data falls into more than one classification, the most restrictive applies, and where classification is unclear, personnel apply Restricted handling until the CISO determines otherwise.

- **Restricted:** Client legal documents and uploaded files; consumer financial data; financial access tokens and credentials; end-client personally identifiable information; and matter metadata revealing the existence or subject of a legal representation. This is the default classification for all customer-supplied content.
- **Confidential:** Law firm account and billing records; internal security documentation including risk registers, incident records, and review findings; production system logs; and source code.
- **Handling of Restricted Data:** Encrypted in transit and at rest as set out in the Access Controls Policy. Stored only within FirmSpan's production environment. Never stored on personal devices, personal cloud storage, or removable media; never transmitted by electronic mail or

consumer messaging platforms; never copied into non-production environments; never submitted to any third-party service, including generative artificial intelligence tools, not approved as a subprocessor; and never written to application or system logs.

4. Retention Schedules

FirmSpan charges on a per-matter basis. Retention operates at both the matter level and the account level, and the earlier applicable period governs.

- **Archived Matters:** All client data associated with a matter, including uploaded documents and financial records, is permanently deleted thirty (30) days after an attorney marks the matter as “archived” within the platform.
- **Maximum Matter Lifecycle:** All client data associated with a matter is permanently deleted nine (9) months after the last activity on that matter, whether or not it has been archived. Activity includes any upload, export, or attorney access. This period runs from last activity rather than matter creation so that a matter which remains active in the underlying representation is not deleted while in use.
- **Account Closure:** If a firm closes its FirmSpan account, the entire workspace — including all remaining client data, database records, and file storage — is permanently deleted sixty (60) days after closure. This period exists to allow export, and export functionality is preserved throughout it.
- **Account Inactivity:** Workspaces with no active matter and no account activity for sixty (60) days are permanently deleted, except while an agreement between FirmSpan and the customer remains in force or a post-termination export window under that agreement remains open.
- **No Extension by Default:** These are fixed platform defaults. FirmSpan does not extend retention for individual matters outside a written agreement executed under Section 8. Where the executed agreement between FirmSpan and the customer provides a longer period for export of customer data, including any post-termination export window, automated deletion under this Section is suspended for the affected data until that period expires; the agreement controls over the schedule above. FirmSpan will notify the customer firm before a matter is deleted under the schedule above, in time to permit export.

5. Customer Export

Attorneys may export all documents and associated metadata for any matter at any time while that matter remains within its retention period, and throughout the sixty-day window following account closure. Exports are delivered in the originally uploaded file formats. Customers are responsible for exercising this capability in advance of the applicable deletion date.

6. Data Disposal

FirmSpan does not use “soft deletion” — hiding data from the user interface while retaining it in the database — for customer files.

- **Hard Deletion:** When an attorney manually deletes a document or client record, or a retention threshold under Section 4 is met, a hard deletion is executed: the file is purged from object storage and the associated relational rows are dropped from the database.
- **Effect of Deletion:** Following hard deletion the data is no longer accessible or recoverable from the active production environment. Residual copies may persist within encrypted backups until those backups age out of the window described in Section 7, after which no copy remains in FirmSpan’s environment.
- **No Secondary Use:** FirmSpan does not retain deleted customer data for analytics, model training, product development, or any purpose other than those described in this policy.

7. Backups and System Logs

Backups and logs operate on schedules separate from customer data retention and are constrained by the capabilities of FirmSpan's managed infrastructure providers. The periods below reflect what is actually achievable under FirmSpan's current production configuration rather than aspirational figures.

- **Database Backups:** Automated daily backups are retained on a rolling seven (7) day basis in encrypted form. Hard-deleted production data may remain within these backups until it ages out of that window.
- **Application and Infrastructure Logs:** Application runtime logs are retained for one (1) day and database, authentication, and storage logs for seven (7) days, as provided by FirmSpan's infrastructure platforms. Identity and source control audit events are retained per those providers' default retention, which exceeds these windows.
- **Acknowledged Limitation:** FirmSpan acknowledges these platform log windows are shorter than the periods commonly expected in vendor security assessments, and shorter than may be required to investigate an incident discovered after a delay. The compensating control is immediate preservation, below.
- **Incident Preservation:** Upon identification of a suspected security incident or receipt of a preservation request, relevant log data is exported from the platform and preserved outside the retention window before it expires. Because the windows are short, preservation is initiated immediately upon identification, in parallel with containment. Preserved logs are stored separately from production and retained for the duration of the investigation and any resulting notification, regulatory, or litigation obligation.

8. Legal Hold and Customer-Specific Requirements

- **Legal Hold:** Upon receipt of a documented legal hold, preservation demand, or lawful process applicable to specific customer data, FirmSpan suspends automated deletion of the affected data for the duration of the hold and notifies the affected customer unless legally prohibited from doing so.
- **Variations by Agreement:** Any variation to the periods in this policy, including extended data or log retention, must be agreed in writing and may be subject to additional fees reflecting the underlying infrastructure cost.

9. Policy Review

This policy is reviewed at least annually by the CISO to ensure alignment with applicable data privacy laws, third-party vendor requirements, and changes to FirmSpan's infrastructure. Section 7 is verified against current provider configuration at each review. This version supersedes all prior versions.