

Information Security Policy

Effective Date: July 27, 2026

Document Owner: Justin Plane, Chief Executive Officer & Chief Information Security Officer (CISO)

1. Purpose and Scope

This policy establishes the framework for safeguarding the information assets, customer data, and operational infrastructure of FirmSpan LLC. It applies to all systems and personnel — including founders, employees, and contractors — operating the FirmSpan application and handling sensitive family law and consumer financial data.

This is the governing document of FirmSpan's security program, supported by the Access Controls Policy, the Data Retention and Disposal Policy, and the Incident Response and Business Continuity Plan.

2. Governance and Responsibilities

- **Chief Information Security Officer:** The CEO, Justin Plane, serves as CISO and holds ultimate responsibility for implementing and enforcing this policy and all subordinate policies. The engineering team is responsible for integrating security practices into the development lifecycle, managing infrastructure access, and participating in quarterly security reviews.
- **Segregation of Duties:** FirmSpan is a small organization in which the CISO also holds executive and engineering responsibilities, so full separation between approver, implementer, and reviewer is not presently achievable. FirmSpan discloses this rather than obscuring it.
- **Compensating Controls:** Production changes are version-controlled and deployed through an automated pipeline, producing an immutable and attributable record; core infrastructure controls are inherited from providers holding independent SOC 2 and ISO/IEC 27001 attestations; administrative access is limited and protected by multi-factor authentication; and quarterly reviews produce written findings independent of individual recollection.
- **Growth Trigger:** Upon FirmSpan employing four or more personnel with production access, security governance will be separated from day-to-day engineering execution, and access reviews will be performed by someone other than the person provisioning access.

3. Infrastructure and Encryption

FirmSpan operates a cloud-native architecture and owns no physical servers, data centers, or network hardware; physical and environmental controls are inherited from its hosting providers. The application frontend and API compute layers run on Vercel (Pro tier), and the relational database and object file storage are managed via Supabase (Pro tier). Both are configured to store and process customer data within the United States. Data is encrypted in transit using TLS 1.2 or higher and at rest using AES-256, covering client legal documents and consumer financial data. Key and secret handling requirements are set out in the Access Controls Policy.

4. Risk Management

- **Risk Register:** FirmSpan maintains a register recording each risk, its likelihood and impact rating, existing controls, the treatment selected, the owner, and the residual risk. Entries are retained a minimum of three years. Risks involving unauthorized disclosure of client legal documents or consumer financial data are rated no lower than High impact by default. Only the CISO may accept a residual risk rated High or above, recorded with a rationale and review date.
- **Cadence:** The register is reviewed at each quarterly security review, with a comprehensive assessment annually. Assessment is also triggered by any security incident, the addition of a

subprocessor handling customer data, or a material change to authorization logic or the data model.

- **Standing Risk Areas:** Cross-tenant access between firm workspaces; compromise of financial integration credentials, consumer financial data, or a privileged administrator account; failure of a critical subprocessor; loss of customer data prior to customer export; and concentration of security responsibility in one individual.

5. Vulnerability and Patch Management

- **Quarterly Security Reviews:** The engineering team audits access, evaluates infrastructure configuration, and assesses emerging threats each quarter. Findings and remediation actions are documented and retained a minimum of two years. GitHub Dependabot performs continuous Software Composition Analysis against application dependencies between reviews.
- **Remediation Targets:** Vulnerabilities are triaged against the targets below, based on CVSS severity. These are targets rather than guarantees; exceptions are documented with a rationale and a compensating control.
- **Critical (CVSS 9.0 – 10.0):** Target remediation within seven (7) days of discovery.
- **High (CVSS 7.0 – 8.9):** Target remediation within thirty (30) days of discovery.
- **Medium and Low (CVSS below 7.0):** Within ninety (90) days, or the next scheduled deployment cycle.

6. Third-Party and Subprocessor Management

FirmSpan's customers remain professionally responsible for ensuring that vendors handling client information act compatibly with the attorney's own duty of confidentiality. This section allows a customer to trace that chain through FirmSpan to its providers.

- **Current Subprocessors:** Vercel (hosting and compute; processes customer data in transit and in memory); Supabase (database, authentication, and file storage; stores customer data at rest); OpenAI (model provider for document verification and assistant features; processes customer data in transit, under API terms that prohibit use of submitted data for model training); Plaid (consumer financial data aggregation); Twilio (transactional electronic mail and SMS notifications to end-clients; processes contact details and notification content, not client documents); Stripe (payment processing for law firm billing; processes firm billing information only, no client data); Google Workspace (internal identity and electronic mail); GitHub (source code management; production customer data is not stored in source control). All subprocessors handling customer data are configured to store and process that data within the United States.
- **Due Diligence:** Before a third party is granted access to customer data or production infrastructure, FirmSpan reviews its security attestations, determines what data it will access and where that data is stored, and reviews its contractual terms. Onboarding requires documented CISO approval. FirmSpan will not onboard a provider whose terms claim ownership of customer data, reserve a right to sell or transfer it, or permit its use for unrelated purposes. FirmSpan will not onboard a model provider absent terms prohibiting the use of submitted customer data to train, fine-tune, or evaluate any model.
- **Monitoring and Notice:** Each subprocessor is reassessed at least annually, and upon any publicly disclosed breach affecting it or material change to its terms or subprocessing arrangements. An incident originating at a subprocessor is handled as a FirmSpan incident where customer data is affected. The list above is FirmSpan's current subprocessor disclosure; advance notice of additions or replacements is provided in accordance with the executed agreement between FirmSpan and the customer.

7. Secure Development and Change Management

- **Environment Separation:** Production customer data is never copied into preview, development, testing, or local environments; development and testing use synthetic or anonymized data. Production secrets are never used in non-production environments.
- **Source Control and Review:** All application code and infrastructure configuration are maintained in GitHub. Changes reach the production branch through a pull request; direct commits are restricted. Committing secrets to source control is prohibited, and any secret so exposed is treated as compromised and rotated. Changes affecting authentication, tenant isolation, authorization logic, data deletion behavior, encryption, or the financial data integration receive explicit security review by the CISO. Where FirmSpan's size means such a change is authored and approved by the same individual, the rationale is recorded and revisited at the next quarterly review.
- **Deployment and Rollback:** Deployments run through a Git-integrated pipeline. Artifacts are immutable and each deployment is retained as a distinct restorable version, constituting FirmSpan's change record. Rollback to the prior known good deployment is the default first response to a defective change. Changes required to contain an incident may be deployed without prior review at the direction of the CISO, and are reviewed retrospectively with the justification recorded.
- **Development Practices:** Authorization, including tenant isolation and role-based permissions, is enforced server-side; client-side controls are never treated as security boundaries. Input is validated and parameterized, uploads are constrained by type and size and stored such that content cannot be executed, and migrations that delete or transform customer data are validated against a non-production restore first.

8. Logging and Monitoring

- **Log Sources:** FirmSpan logs application authentication and session events, document upload and download events, administrative actions, platform and database activity, identity and source control audit events, and financial integration calls sufficient to reconstruct what was requested and when.
- **Prohibited Log Content:** Credentials, session or access tokens, magic link tokens, financial integration secrets, full financial account numbers, and the contents of client documents must never be written to any log in any environment. Prohibited content found in a log is reported as a security incident.
- **Monitoring:** Access logs, authentication anomalies, and administrative actions are reviewed at each quarterly security review, and automated infrastructure and dependency alerts are triaged by the CISO on receipt. Reviews give specific attention to failed authentication patterns, magic link anomalies, patterns suggesting attempted cross-tenant access, unexpected privilege changes, and anomalous volumes of document access or export. Log retention and incident preservation are set out in the Data Retention and Disposal Policy.

9. Personnel Security and Acceptable Use

Acknowledgment of this section is a condition of receiving access to FirmSpan systems, renewed annually.

- **Onboarding:** Personnel granted access to production environments or customer data complete security and data privacy training and execute a written confidentiality agreement with FirmSpan before access is granted. FirmSpan conducts background checks on personnel engaged beyond the founding team; the founders have not been subject to third-party background screening, and FirmSpan discloses this rather than implying a control it does not operate.
- **Authentication:** Multi-factor authentication is required on every account with access to FirmSpan infrastructure, source control, identity services, or customer data, using authenticator

applications or hardware keys. Passwords must be long, unique per service, and stored in a password manager. Credential sharing and shared accounts are prohibited.

- **Devices:** Devices used to access FirmSpan systems must have full-disk encryption, a supported and current operating system, an active firewall, real-time anti-malware protection, and an automatic screen lock. They must not be left unattended in unsecured locations or shared with third parties while FirmSpan credentials are accessible, and loss or theft must be reported immediately.
- **Data Handling:** Customer data must not be downloaded to personal storage, cloud accounts, removable media, or personal electronic mail; must not be copied into non-production environments; and must not be submitted to any generative artificial intelligence service or other tool not approved as a subprocessor under Section 6.
- **Prohibited Conduct:** Accessing customer data without a legitimate business need, including viewing client documents out of curiosity; disclosing customer data or the existence of a client matter to a third party; circumventing security controls; and retaining customer data or confidential material after the end of engagement.
- **Reporting and Enforcement:** Personnel must promptly report any suspected incident, phishing attempt, unauthorized access, or policy violation to the CISO. Good-faith reports will not result in adverse consequences for the reporting individual, including where the report concerns their own error. Violation may result in revocation of access, termination of engagement, and referral to law enforcement where the conduct is unlawful.

10. Processor Role and Customer Assurance

- **Processor Status:** FirmSpan acts as a Data Processor on behalf of its law firm customers, who act as Data Controllers with respect to client data, and processes customer data only on the customer's documented instructions and as necessary to deliver the service.
- **Data Ownership:** Customer data, including all client materials uploaded to the platform, remains the property of the law firm and its clients. FirmSpan asserts no ownership interest, does not sell or license customer data, and does not use customer content to train machine learning models.
- **Contractual Commitments:** Binding commitments are made through the executed written agreement between FirmSpan and the customer. These policies are supporting evidence of FirmSpan's control environment, not customer contracts.

11. Policy Review

This policy is reviewed at least annually by the CISO, or following any significant change to FirmSpan's infrastructure, business operations, or regulatory obligations. This version supersedes all prior versions.