

Access Controls Policy

Effective Date: July 27, 2026

Document Owner: Justin Plane, Chief Executive Officer & CISO

1. Purpose and Scope

This policy defines the requirements for managing access to FirmSpan LLC's networks, systems, applications, and data, and for protecting the credentials and cryptographic material that secure them. It enforces least privilege and strict data segmentation between law firm customers.

2. Internal Access and Privileges

- **Centralized Identity:** Google Workspace serves as the central directory and identity provider for authenticating internal personnel to company tools and third-party services.
- **Administrative Privileges:** The core engineering team holds administrative privileges across Vercel, Supabase, GitHub, and the Plaid Dashboard, granted only to personnel with a documented operational need.
- **Authentication:** All administrative and infrastructure platforms require strong, unique passwords and enforced Multi-Factor Authentication. Shared or generic accounts are prohibited; every individual holds a uniquely attributable identity.

3. Application Access and RBAC

Access to the FirmSpan application is governed by Role-Based Access Control, separating permissions between legal professionals and their clients, and between distinct law firm workspaces.

- **Tenant Segmentation:** Each law firm workspace is logically segregated. Authorization is enforced server-side, and no user may access data belonging to another firm's workspace.
- **Attorney Access:** Attorneys authenticate via email and password, and may view, manage, export, and download documents associated solely with their own clients. Multi-Factor Authentication is not currently enforced on attorney accounts. FirmSpan discloses this rather than implying a control it does not operate. Attorney accounts require strong, unique passwords; authorization and tenant isolation are enforced server-side and are unaffected by this; and failed authentication patterns and anomalous document access are reviewed as set out in the Information Security Policy. Enforcement of Multi-Factor Authentication on attorney accounts is tracked as an open item in FirmSpan's risk register and is reviewed at each quarterly security review.
- **Client Access:** End-clients authenticate using secure, single-use magic links. The client portal enforces stateless sessions and does not retain financial login states between sessions. Compromise of a magic link does not grant access to historical data or previously established sessions.
- **Client Data Restrictions:** Clients hold upload-only permissions by design. The application does not permit end-clients to view, download, or retrieve previously uploaded documents, financial records, or data payloads. This intentional design decision reduces the exposure surface of uploaded material; the attorney, as Data Controller, retains the ability to release documents to their client through their own channels.

4. Secrets, Keys, and Encryption

- **Secrets Management:** All production secrets, database credentials, and third-party API keys are stored encrypted within Vercel's environment variable manager and injected into the runtime at execution. Secrets are never present in source code or deployment artifacts, and never stored in plaintext files, electronic mail, instant messages, shared documents, or personal notes applications.

- **Service Authentication:** Non-human authentication for internal services and third-party integrations, including Plaid, relies on managed OAuth tokens and scoped API keys granted the minimum product access necessary.
- **Encryption in Transit:** All data transmitted between end users and FirmSpan, and between FirmSpan and its subprocessors, is encrypted using TLS 1.2 or higher. The application is served exclusively over HTTPS with HTTP Strict Transport Security enabled. Certificate validation must never be disabled in any environment handling production credentials or customer data.
- **Encryption at Rest:** Customer data at rest, including client legal documents, uploaded files, consumer financial data, and all database contents, is encrypted using AES-256. Encryption at rest and the underlying key management infrastructure are provided by the Supabase platform; FirmSpan does not operate its own key management service.
- **Plaid Credentials:** Plaid client secrets are stored exclusively as production environment variables and are never transmitted to the client browser or written to logs. Plaid access tokens are stored encrypted at rest and are invalidated and destroyed when the associated matter's data is deleted under the Data Retention and Disposal Policy.
- **Rotation:** Secrets are rotated immediately upon any suspicion of exposure, including exposure in source control, in logs, or on a lost or stolen device; upon the departure of any individual with access to them; upon termination of a vendor relationship; and at least annually where the platform supports rotation without service disruption. Suspected exposure is treated as actual exposure, and each rotation is recorded with the date, the secret rotated, and the reason.
- **Prohibited Practices:** Protocols or cipher suites below TLS 1.2; unsalted or fast hash functions for password storage; custom cryptographic algorithms in place of established libraries; and hardcoded secrets in application code, container images, or client-side bundles.

5. Lifecycle Management and Zero Trust

- **Zero Trust Posture:** Every access request, human or automated, must be authenticated and authorized against defined IAM policies before access is granted to FirmSpan resources or the Plaid API. No implicit trust is granted based on network location or device ownership.
- **Provisioning:** Access is provisioned on least privilege, with elevated permissions granted only for the duration of a documented need.
- **Offboarding:** Upon termination of an employee or contractor, de-provisioning is initiated immediately through Google Workspace, followed by manual revocation of platform-specific access. FirmSpan's target is complete revocation of access to APIs, services, the codebase, and customer data within twenty-four (24) hours of termination, and no later than the next business day. Secrets accessible to the departing individual are rotated as part of this process.

6. Access Reviews

Internal access privileges, active accounts, RBAC configurations, third-party integrations, and long-lived credentials are reviewed during quarterly security reviews. Anomalous, dormant, or excessively privileged accounts are modified or revoked. Each review produces a written record identifying the accounts reviewed, the reviewer, the date, and any actions taken. These records are retained a minimum of two (2) years and are available to customers under an executed non-disclosure agreement. FirmSpan's documented security program commenced on the effective date of this policy; records exist from that date forward.

7. Policy Review

This policy is reviewed at least annually by the CISO, or following any significant change to FirmSpan's identity architecture, application authorization model, or infrastructure providers. This version supersedes all prior versions.