

Incident Response and Business Continuity Plan

Effective Date: July 27, 2026

Document Owner: Justin Plane, Chief Executive Officer & CISO

1. Purpose and Scope

This plan defines how FirmSpan LLC detects, contains, investigates, and reports security incidents, and how it restores service following a disruptive event. It applies to all personnel and to any event affecting the production environment, customer data, or the confidentiality of client legal or consumer financial information.

A security incident is any actual or reasonably suspected event that compromises, or threatens to compromise, the confidentiality, integrity, or availability of FirmSpan systems or customer data.

2. Roles

- **Incident Commander:** The CISO, Justin Plane, holds authority to direct containment, engage external counsel or forensic support, and authorize customer and regulatory notification.
- **Alternate Contact:** Because the Incident Commander role is held by one individual, FirmSpan maintains a documented alternate with authority to initiate containment if the CISO is unreachable, and ensures the credentials and recovery methods needed to restore service are accessible to more than one person.
- **External Support:** Where an incident exceeds internal capability, the Incident Commander engages external forensic and legal support, identified in advance of need.

3. Response

- **Identification:** Incidents are identified through anomaly detection in platform logs, automated vulnerability alerts, customer or end-user reports, third-party notification including from a subprocessor, or internal discovery. The Incident Commander is notified without delay and an incident record is opened.
- **Evidence Preservation:** In any incident involving suspected unauthorized access to customer data, and before any containment action that would destroy evidence, relevant logs are exported and preserved outside the platform retention windows described in the Data Retention and Disposal Policy. Because those windows are as short as one day, preservation is the first documented action after identification and runs in parallel with containment.
- **Containment:** The Incident Commander authorizes measures proportionate to the threat, which may include revoking compromised credentials, rotating API keys including financial integration secrets, invalidating active sessions and magic links, isolating affected database instances, blocking network sources, or temporarily suspending the application. Containment takes priority over investigation.
- **Eradication and Recovery:** Root cause is determined, the underlying vulnerability or misconfiguration is remediated, elimination of unauthorized access is validated, and affected services are restored in accordance with Sections 5 and 6.
- **Post-Incident Review:** Following resolution of any incident involving confirmed or suspected unauthorized access to customer data, the CISO produces a written review recording the timeline, root cause, customer impact, actions taken, and corrective actions with owners. Corrective actions are tracked in the risk register.

4. Notification

An incident is reportable where it involves confirmed or reasonably suspected unauthorized access to, or acquisition of, customer data. Reportable incidents are escalated immediately and trigger the obligations below; all other events are handled through ordinary remediation and recorded in the incident record. FirmSpan does not delay notification pending complete investigation where the facts establish a reportable event.

- **Customers:** FirmSpan notifies affected law firm customers without undue delay following determination of the scope of compromise, and in any event within the timeframe required by applicable law. FirmSpan targets initial notification within seventy-two (72) hours of confirming a reportable breach where the facts reasonably permit. Notification includes the nature of the incident, the categories of data affected, the measures taken, and a point of contact.
- **Controller Responsibility:** As Data Processor, FirmSpan notifies the law firm as Data Controller. Any obligation to notify the firm's own clients rests with the firm, and FirmSpan will provide the information reasonably necessary for the firm to discharge it.
- **Partners:** Financial data and other critical integration partners are notified within the timeframes required by their respective agreements where an incident affects consumer financial data or the integrity of the integration.
- **Regulators:** Where applicable state or federal law requires notification to a regulator or state attorney general, FirmSpan complies within the statutory deadline. State deadlines to affected individuals currently range from approximately thirty (30) to sixty (60) days, and FirmSpan's processes are designed to meet the shortest applicable deadline.
- **Communications Discipline:** All external communications regarding an incident are approved by the Incident Commander.

5. Recovery Objectives and Backups

FirmSpan operates no physical infrastructure, and its resilience posture is substantially inherited from its providers. This section states plainly which capabilities are FirmSpan's and which are its providers'.

- **Recovery Point Objective:** Up to twenty-four (24) hours, reflecting reliance on automated daily backups. Data written after the most recent daily backup may be unrecoverable in a total database loss scenario.
- **Recovery Time Objective:** Twenty-four (24) hours for restoration of core application functionality from backup following total loss of the production database.
- **Backups:** Automated daily database backups are retained on a rolling seven-day basis in encrypted form. Application source code and infrastructure configuration are maintained in version control, enabling reconstruction of the application layer independently of the hosting provider. A backup that has not been restored is not treated as a proven backup; restoration is validated at least annually.
- **Objective Review:** These objectives are reviewed annually against customer expectations and infrastructure capability. Where a customer requires a shorter Recovery Point Objective, FirmSpan will address that contractually, including through provisioning of point-in-time recovery capability at additional cost.

6. Disruption Scenarios

- **Defective Deployment:** Roll back to the last known good deployment; recovery is measured in minutes and is the first response to a defective change.
- **Database Corruption or Data Loss:** Assess scope, halt writes if necessary, restore from the most recent valid daily backup, validate integrity, and communicate any residual data loss to affected customers.

- **Provider Outage:** FirmSpan monitors provider status channels and communicates status to affected customers. FirmSpan does not currently maintain a secondary hosting provider capable of independent failover, and states this rather than implying a capability it does not have.
- **Loss of Administrative Access:** Recovery proceeds through the provider's documented account recovery process using pre-established recovery methods.
- **Loss of Financial Data Integration:** Degrades data collection functionality without affecting the confidentiality or integrity of data already held.

7. Testing and Customer Communication

- **Annual Testing:** FirmSpan restores a database backup to a non-production environment at least annually and validates data integrity, and conducts a tabletop walkthrough of at least one incident scenario against this plan. Results and any deficiencies are recorded.
- **Plan Availability:** This plan is stored such that it remains accessible during an incident affecting FirmSpan's primary production environment.
- **Status Communication:** During a disruption materially affecting availability, FirmSpan communicates the nature of the disruption, expected restoration, and any known data impact to affected customers. Where recovery results in loss of customer data, FirmSpan notifies each affected customer identifying the period and categories of data affected.

8. Policy Review

This plan is reviewed at least annually by the CISO, following any reportable incident, following any actual invocation of the continuity provisions, and following any material change to FirmSpan's infrastructure or notification obligations.