Incident Response Plan

How we detect, contain, and communicate about security incidents that affect customer data.

Last updated May 29, 2026

Scope

This plan describes how Notion State responds to security incidents that affect the Notion Scan service, customer data, or the systems that support them. It covers detection, triage, containment, customer notification, and post-incident review.

A security incident is any unauthorized access to, disclosure of, modification of, or loss of customer data, or any compromise of the systems that store or process customer data.

Severity classification

We classify incidents into three levels:

Level	Definition	Initial response time
Critical	Confirmed unauthorized access to or disclosure of customer data; service-wide outage; compromise of authentication or encryption infrastructure.	Within 4 hours of detection
High	Suspected unauthorized access; partial service degradation affecting multiple customers; loss of integrity of customer data.	Within 1 business day of detection
Moderate	Single-customer impact with no data disclosure; isolated service issue; suspected but unconfirmed indicator of compromise.	Within 3 business days of detection

Severity is assigned at triage and revised as more information becomes available.

Detection sources

We rely on a combination of signals to detect incidents:

- Application logs and error reporting.
- Database query monitoring and anomaly detection via Supabase.
- Authentication provider alerts.
- Customer-reported issues sent to security@notionscan.com.
- Subprocessor breach notifications.

Triage workflow

When a potential incident is detected:

1. **Acknowledge.** The Head of Engineering acknowledges the alert and records the time of detection.
2. **Classify.** Severity is assigned based on the criteria above.
3. **Activate.** For Critical or High incidents, the Head of Engineering is alerted via Slack and the response begins immediately; for Moderate, response proceeds during business hours.
4. **Investigate.** Logs, traces, and database state are reviewed to determine scope, root cause, and affected customers.
5. **Document.** Findings are recorded in an incident timeline as they emerge.

Containment

Containment actions vary by incident type. Standard actions include:

- Revoking compromised credentials or session tokens.
- Disabling affected API routes or background jobs.
- Rotating encryption keys for affected resources.
- Removing or quarantining anomalous data.

- Isolating affected infrastructure components from the network.

Customer notification

For incidents that affect customer data, we notify affected customers:

- **Critical incidents:** within **72 hours** of confirming impact.
- **High incidents:** within **5 business days** of confirming impact.
- **Moderate incidents:** in the next regular service communication, with a description of impact and remediation.

Notification is sent to the customer's primary contact and includes:

- A description of the incident.
- The types of data affected.
- Actions we have taken to contain and remediate.
- Recommended actions for the customer.
- A contact for follow-up questions.

Post-incident review

For every Critical or High incident, we conduct a post-incident review within **10 business days** of resolution. The review documents:

- Timeline of events from detection to resolution.
- Root cause.
- What worked and what did not.
- Specific changes to prevent recurrence (code, configuration, process).

A summary of post-incident reviews is shared with affected customers on request.

Roles and responsibilities

The response covers the following functions:

- **Incident Commander, Engineering Lead, and Security Contact.** Owns the response end to end: triage, technical containment and remediation, root cause investigation, and liaison with regulators, subprocessors, and external counsel where applicable.
- **Communications Lead.** Drafts customer and internal updates and coordinates external notifications.

These responsibilities are assigned internally and reviewed as roles change.

Customer support during incidents

Customers can reach us at security@notionscan.com during an incident. We aim to respond to incident-related inquiries within 4 business hours during active Critical incidents.

Review

This plan is reviewed annually and after every Critical incident. The `Last updated` date at the top of this page reflects the most recent revision.