Information Security Policy

The umbrella policy that governs how Notion State protects customer data, including governance, classification, and review cadence.

Last updated May 29, 2026

Purpose

This policy sets the framework under which Notion State protects the confidentiality, integrity, and availability of customer data processed by the Notion Scan service. It defines the responsibilities, controls, and review cadence that underpin our security posture.

This policy is the umbrella document. The specific controls and procedures are documented in the other policies linked throughout.

Scope

This policy applies to:

- All Notion Scan systems, including application code, infrastructure, databases, and integrations.
- All Notion State personnel, contractors, and authorized third parties who access these systems.
- All customer data processed by the service.

Governance

The Notion State leadership team owns this policy. The Head of Engineering is the designated security owner and is responsible for:

- Maintaining and reviewing this policy and the linked policies.

- Coordinating responses to security events per the Incident Response Plan.
- Reviewing access grants, subprocessor changes, and material architecture changes.

Material changes to security posture require leadership approval and are reflected in the Trust Center.

Information classification

We classify the information we hold into three tiers. Controls scale with sensitivity.

Tier	Examples	Handling
Restricted	Encrypted Notion integration tokens, encryption keys, customer account credentials	Encrypted at rest; access strictly limited; never logged in plaintext
Confidential	Workspace metadata, scan snapshots, derived analysis	Stored in tenant-isolated database; access via authenticated client scope only
Internal	Operational logs, application metrics, aggregated analytics	Retained for limited windows; reviewed for security-relevant patterns

Customer workspace data is handled as Confidential or Restricted depending on sensitivity. We do not rely on a lower "public" classification for customer workspace metadata, even when a customer's workspace contains public-facing or marketing-related material.

Access control principles

- **Least privilege.** Personnel and systems are granted the minimum access required to perform their function.
- **Authentication.** Access to customer data requires authenticated sessions backed by our auth provider.

- **Authorization.** Role-based controls enforce what each user or service account may do. Cross-tenant access requires the explicit `admin` role.
- **Token security.** Notion integration tokens are encrypted at rest with AES-256-GCM; details in the Security Overview.
- **Customer isolation.** Application-layer authorization constrains every request to the user's authorized client scope, with Postgres Row-Level Security as a defense-in-depth backstop; details in the Customer Isolation Policy.

Operational security

- **Code review.** Changes to systems that handle customer data are reviewed before merge.
- **Dependency management.** Third-party packages are tracked, patched, and audited for known vulnerabilities.
- **Infrastructure hardening.** Production systems run on hosted platforms (Vercel, Supabase, Railway) with their default security baselines, supplemented by application-level controls including a strict Content Security Policy, HSTS, frame-ancestor restrictions, and input validation at trust boundaries.
- **Secrets management.** Application secrets are stored in encrypted environment variables, scoped per environment, and never committed to source control.

Logging and monitoring

- Authentication events are logged by our auth provider; scan worker activity is logged with scan identifiers and timestamps.
- Operational logs are generated and retained by our infrastructure providers (Vercel, Railway, Supabase), each per its own retention schedule; we do not keep a separate copy. We review them for security-relevant anomalies within those windows.
- Customer-reported security concerns are escalated per the Incident Response Plan.

Vendor and subprocessor management

We use a limited set of subprocessors, listed and described in the Subprocessors document. New subprocessors are reviewed for:

- Security posture (certifications, public security documentation).
- Data residency and data flow implications.
- Contractual terms aligned with our confidentiality, security, and data protection obligations.

Material changes to subprocessors are communicated to customers in advance per the Subprocessors policy.

Data handling

- **What we collect, store, and never store** is documented in the Security Overview and Privacy Policy.
- **Retention and deletion** are governed by the Data Retention Policy.
- **Customer isolation** is enforced as described in the Customer Isolation Policy.

Personnel

- Personnel with access to production systems are bound by confidentiality obligations.
- Access is reviewed when roles change or personnel leave.

Compliance posture

We have not yet completed SOC 2 Type II or ISO 27001 certifications. We operate on infrastructure that holds relevant third-party security attestations (Vercel, Supabase, and Railway) and our controls are designed to align with the corresponding trust services criteria.

Review

This policy is reviewed at least annually and after any material change in our product, infrastructure, or threat model. The `Last updated` date at the top of this page reflects the most recent revision.

Contact

Security questions, vulnerability reports, or policy clarifications: security@notionscan.com.