



REGULACORE

Security & Trust Whitepaper

Current architecture, safeguards, assurance status, and customer responsibilities

VERSION	1.0
PUBLISHED	July 27, 2026
OWNER	RegulaCore Security & Privacy

Evidence-backed transparency for enterprise security and procurement review.

1. Executive Summary

RegulaCore provides a multi-tenant platform for EHS, quality, ISO readiness, training, audit, and compliance workflows. This document separates implemented architecture from provider capabilities and future assurance work. It is intended to help security and procurement teams begin a factual review.

RegulaCore does not claim a certification, audit report, service level, or test result unless the underlying document has been issued and made available for qualified review.

Current assurance status

Topic	Current public status
SOC 2	Readiness roadmap. No SOC 2 Type II report is represented as issued.
ISO/IEC 27001	Alignment roadmap. RegulaCore is not represented as certified.
Independent penetration test	No report is represented as available until an assessment is completed.
HIPAA-regulated use	No HIPAA certification is claimed. PHI use requires written review and an approved BAA.

2. Architecture

The inspected production architecture is Cloudflare-native. Cloudflare provides the global edge and managed platform services; RegulaCore is responsible for secure application design, configuration, authorization, and customer-data handling.

Service	RegulaCore use	Security boundary
Cloudflare Workers	Application and API compute	Edge execution and deployment configuration
Cloudflare D1	Relational application records	Shared multi-tenant tables with tenant-scoped queries
Cloudflare R2	Documents and evidence objects	Tenant-namespaced object keys and authorized access
Cloudflare KV	Selected configuration, cache, and session support	Binding-level access and application controls
Durable Objects	Selected coordinated state	Binding-level access and service-specific authorization

Provider encryption

Cloudflare documents AES-256 encryption at rest for D1 and R2. HTTPS terminates at Cloudflare's edge. Encryption protects stored and transmitted data; it is not a substitute for tenant authorization.

3. Tenant Isolation and Access

RegulaCore uses a shared multi-tenant model. It does not currently describe each customer as having a dedicated database. Tenant separation is enforced through authenticated context, authorization checks, tenant identifiers on customer-owned records, tenant-scoped queries, and tenant-namespaced storage keys.

- Protected API requests must present a verified tenant or administrator session.
- Tenant-owned database queries bind the authenticated tenant identifier.
- Administrative and tenant authorization realms are kept distinct.
- Missing authentication secrets fail closed; predictable development-secret fallbacks are prohibited.
- Endpoint authorization and cross-tenant regression checks are treated as release gates.

Customer responsibilities

- Manage authorized users, roles, and prompt deprovisioning.
- Configure retention and workflow controls appropriate to the customer's legal obligations.
- Do not upload regulated data outside the scope approved in the service agreement.
- Report suspected account compromise or vulnerabilities promptly.

4. Network and Browser Safeguards

- HTTPS is enforced at Cloudflare's edge and supported clients negotiate modern TLS.
- Cloudflare provides network-layer DDoS protections. WAF status is verified from production configuration rather than inferred from hosting alone.
- Marketing responses use HSTS, anti-framing, MIME-sniffing protection, referrer controls, and a permissions policy.
- The Security & Trust page has an enforced Content Security Policy. Legacy marketing pages begin with report-only monitoring before enforcement.

5. Secure Development

RegulaCore's secure-development program prioritizes secret management, authenticated-by-default API behavior, tenant-scoped access, parameterized queries, dependency review, vulnerability intake, and evidence-producing release checks. Controls described as automated are not presented as operating until the automation and retained evidence can be demonstrated.

6. Logging, Retention, and Recovery

Supported workflows record tenant-scoped operational and audit events. Current D1 records are not described as immutable or tamper-proof. Append-only and tamper-evidence capabilities remain assurance-roadmap items.

Retention, availability, recovery time, and recovery point commitments depend on product configuration and the signed service agreement. Cloudflare D1 recovery capabilities depend on the active plan and database version and are verified before contractual commitments are made.

7. Incident Response and Disclosure

- Security reports are received at support@regulacore.com.
- Reports are triaged according to severity, exploitability, customer impact, and scope.
- Affected customers are notified without undue delay as required by applicable law and the DPA.
- Root-cause analysis and corrective actions are tracked for material incidents.

Responsible disclosure policy: <https://regulacore.com/security#responsible-disclosure>

Security contact file: <https://regulacore.com/.well-known/security.txt>

8. Procurement Evidence

Artifact	Access
Security & Trust page	Public: https://regulacore.com/security
Security Whitepaper	Public, versioned PDF
Data Processing Addendum	Public HTML and PDF; countersignature by request
Subprocessor list	Published in the DPA
Non-public evidence	Qualified request to support@regulacore.com ; NDA where appropriate

9. External References

Cloudflare D1 data security: <https://developers.cloudflare.com/d1/reference/data-security/>

Cloudflare R2 data security: <https://developers.cloudflare.com/r2/reference/data-security/>

Cloudflare SaaS data-isolation patterns: <https://developers.cloudflare.com/use-cases/saas/data-isolation/>

Cloudflare D1 Time Travel: <https://developers.cloudflare.com/d1/reference/time-travel/>

Contact

Security, privacy, and DPA: support@regulacore.com

RegulaCore Inc., 500 Navarro St, 2nd Floor, PMB 7096, San Antonio, TX 78205, United States