SECURITY & COMPLIANCE WHITE PAPER

Fabrication Pro

Security & Compliance Architecture

Data Protection · Infrastructure Boundaries · GovCloud Readiness

---

AWS · GitHub · Cloudflare · GCP KMS · AI Gateway

Prepared for: Fabrication Pro Clients

May 2026 · Version 1.0

FedRAMP / GovCloud Readiness Reference · NIST 800-53 · ISO 27001 · SOC 2 Type II

Executive Summary

Fabrication Pro is built on a multi-cloud, enterprise-grade infrastructure stack purpose-designed for security, data sovereignty, and regulatory compliance. This document provides clients, IT security teams, and procurement professionals with a definitive reference to how Fabrication Pro protects your data, where it lives, who can access it, and the path toward full GovCloud authorization.

Fabrication Pro does not rely on proprietary databases or opaque infrastructure. Every underlying technology is an open standard operated by independently audited cloud providers. This means your data, your code, and your business logic are always portable and never locked in.

Fabrication Pro Security Posture

SOC 2 Type II certified (August 2025) · ISO 27001:2022 certified · GDPR compliant · EU AI Act Low Risk. All data is encrypted with AES-256 at rest and TLS 1.3 in transit. Fabrication Pro is on a documented path to FedRAMP / GovCloud authorization.

What This Document Covers

- The full seven-zone infrastructure architecture with provider-level detail
- How every user request flows through security checkpoints before data is accessed
- The three-layer encryption architecture protecting data at transport, application, and storage
- Compliance certifications and regulatory alignment (GDPR, CCPA, NIST 800-53, FedRAMP)
- The GovCloud readiness roadmap for government and defense clients
- Recommended client-side security configuration

Platform Architecture Overview

Fabrication Pro’s infrastructure is organized into seven security zones, each operated by a distinct cloud provider with its own compliance certifications, access controls, and audit trail. The zones work in concert but are independently auditable — a failure or compromise in any single zone does not compromise the others.

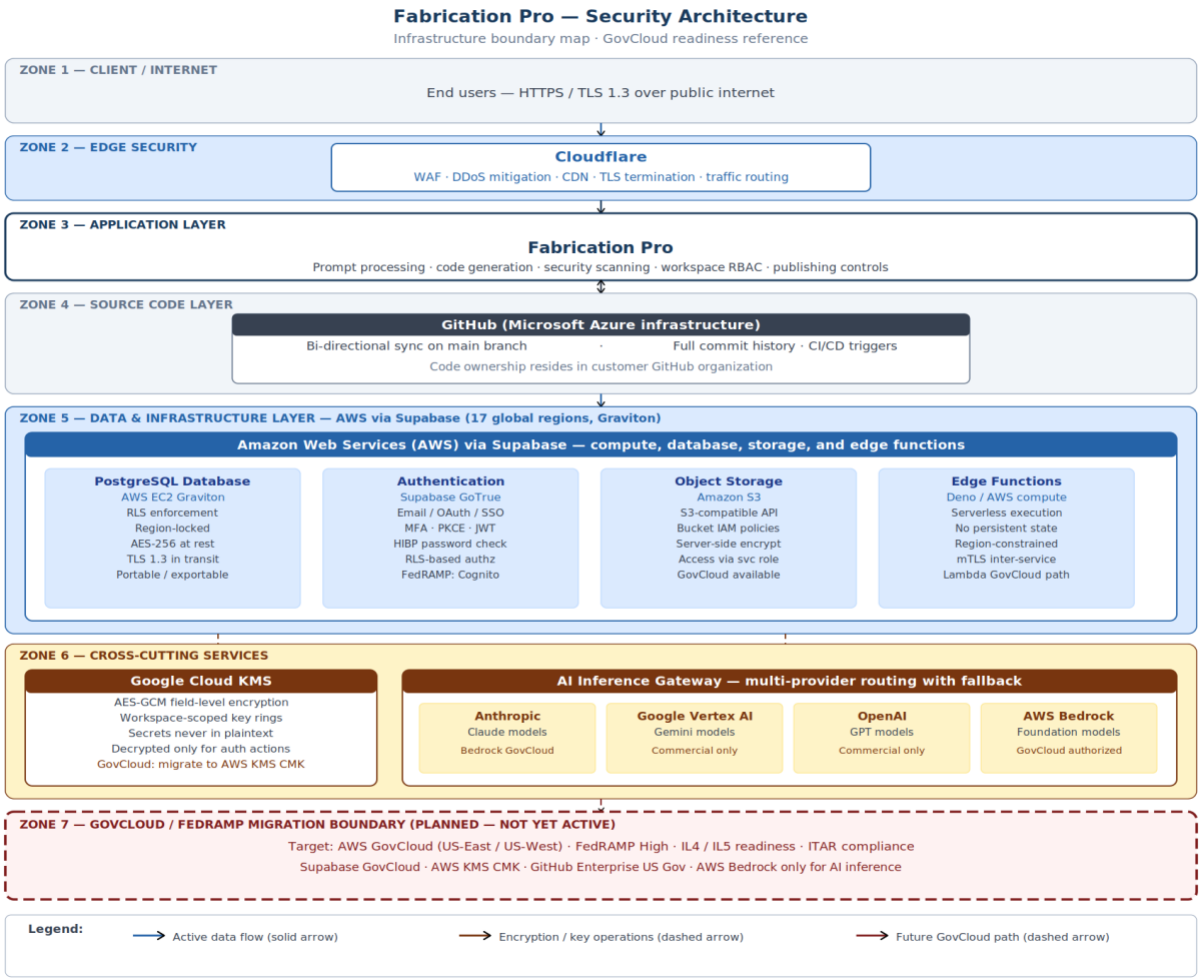

Figure 1: Fabrication Pro — Full Security Architecture. Seven zones from client edge through the planned GovCloud migration boundary.

No Single Point of Failure

Fabrication Pro's architecture is designed so that no single provider holds all of your data. Application code lives in your GitHub organization. Application data lives in AWS. Encryption keys live in Google Cloud KMS. Compromising any single zone does not yield readable data — an attacker would need to breach AWS, GCP, and your GitHub organization simultaneously.

Request Lifecycle & Security Checkpoints

Every request to Fabrication Pro — from loading the dashboard to submitting a production order — passes through multiple security checkpoints before any data is accessed or returned. No request reaches your database without traversing all of these controls.

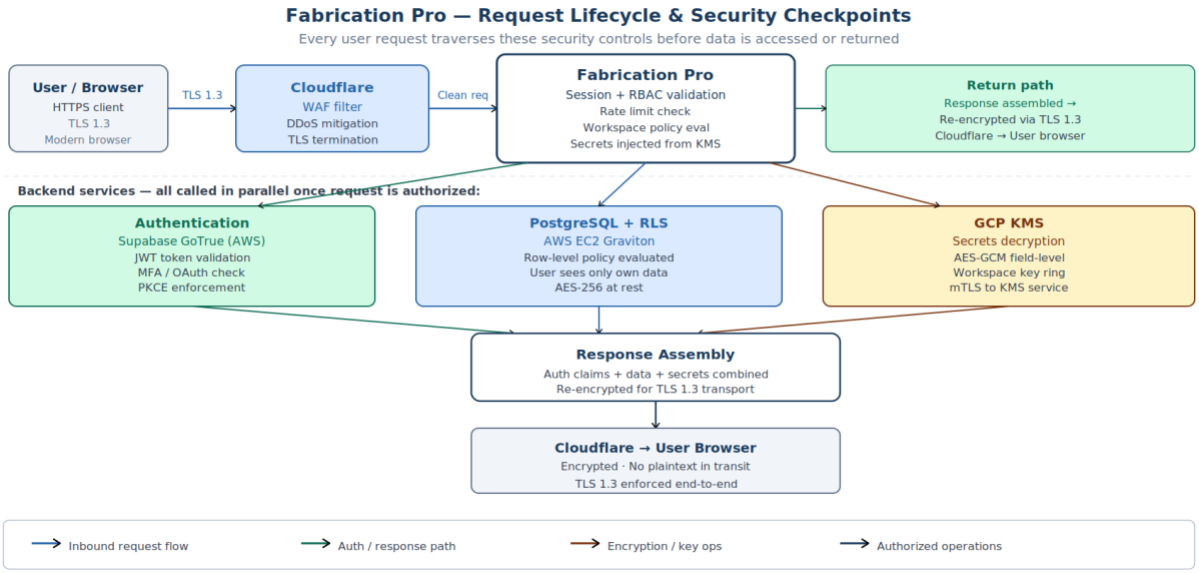

Figure 2: Fabrication Pro — Request Lifecycle. Every user request traverses WAF, RBAC, authentication, RLS policy evaluation, and encrypted response assembly before data is returned.

Security Checkpoints in Order

1. TLS 1.3	All connections are encrypted the moment they leave the user's browser. TLS 1.3 with perfect forward secrecy is enforced — downgrade to older TLS versions is blocked
2. Cloudflare WAF	Every request passes through Cloudflare's Web Application Firewall, which filters OWASP Top 10 attacks, SQL injection, XSS, DDoS, and malformed requests before they reach any Fabrication Pro server
3. Rate Limiting	Adaptive rate limiting at IP, user, and workspace level prevents brute force, credential stuffing, and abuse
4. RBAC Evaluation	Fabrication Pro evaluates the authenticated user's role before any operation. Editing, approving, and publishing are separate permissions enforced server-side — not client-side
5. Authentication Check	Supabase GoTrue validates the session JWT, checks MFA status, and confirms the session has not expired or been revoked
6. Row Level Security	Every database query is evaluated against RLS policies inside PostgreSQL. Users can only read and write records they are authorized to access — even if a query is crafted to bypass the application layer
7. Secrets Decryption	API keys and credentials needed for the operation are decrypted from GCP KMS only at the moment they are needed, and only for authorized integrations. They are never logged
8. Encrypted Response	The assembled response is encrypted in transit via TLS 1.3 through Cloudflare back to the user's browser. No plaintext data exists at any

	point in the network path

Encryption Architecture

Fabrication Pro protects your data with three independent encryption layers. These layers operate simultaneously and independently: if any single layer were somehow compromised, the other two would still protect your data. This ‘defence in depth’ approach is the industry gold standard.

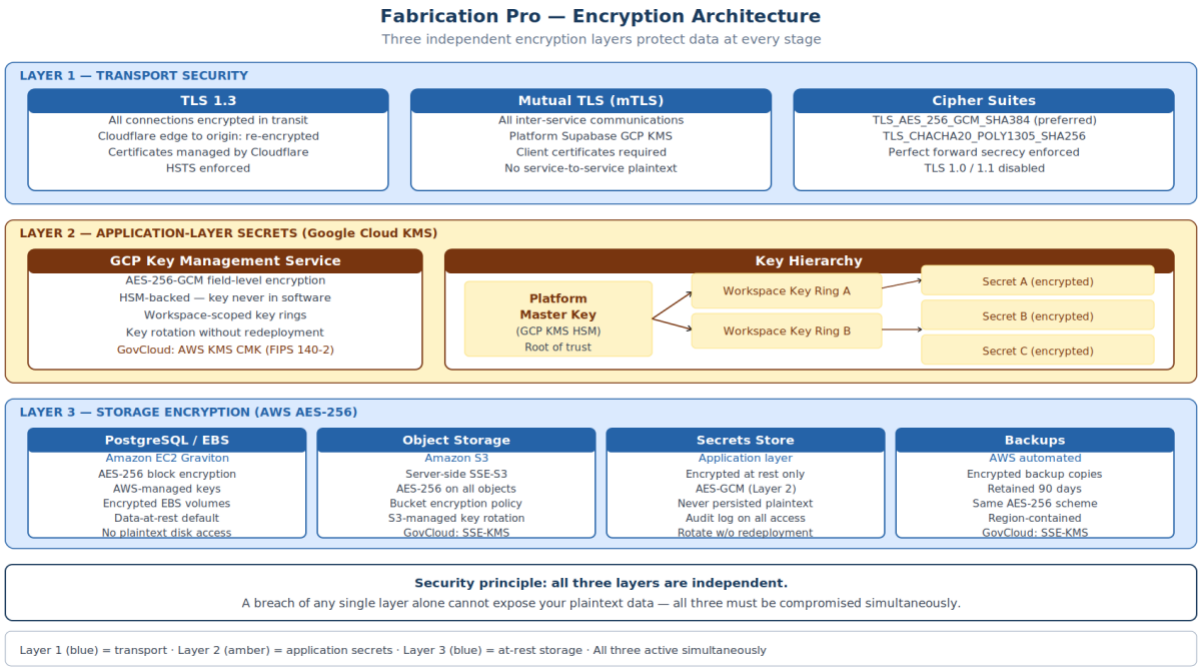

Figure 3: Fabrication Pro — Three-Layer Encryption Architecture. Transport (TLS 1.3 / mTLS), Application (GCP KMS AES-GCM), and Storage (AWS AES-256) layers operate independently.

Layer	Technology	Protection Scope
Layer 1 — Transport	TLS 1.3 + mTLS	All data in transit between user, Cloudflare, Fabrication Pro, and backend services. Perfect forward secrecy on every session. Mutual TLS for all inter-service communication
Layer 2 — Application	AES-GCM via GCP KMS	All secrets, API keys, and credentials. Field-level encryption with workspace-scoped key rings. Master key held in Google Cloud HSM. Decrypted only for authorized operations
Layer 3 — Storage	AES-256 on AWS	All data at rest in PostgreSQL (encrypted EBS volumes) and Amazon S3 (SSE-S3). Encryption is automatic and cannot be disabled. AWS-managed keys with GCP KMS

		overlay for secrets

Encryption Key Management

Fabrication Pro manages encryption keys through a hierarchical structure designed to provide tenant isolation while maintaining operational efficiency. Your workspace has its own dedicated key ring within Google Cloud KMS, meaning another customer's key material can never decrypt your data.

Key algorithm	AES-256-GCM — authenticated encryption that simultaneously encrypts and verifies data integrity
Key storage	Google Cloud HSM (Hardware Security Module) — the master key never exists in software
Key isolation	Workspace-scoped key rings — each Fabrication Pro workspace has dedicated keys
Key rotation	Secrets can be rotated at any time without service redeployment or data loss
Audit trail	All key access and decryption events are logged with timestamp, operation, and requesting service
GovCloud path	For government deployments: AWS KMS Customer Managed Keys with FIPS 140-2 Level 2 HSMs

Infrastructure Zone Detail

Zone 1 — Client / Internet

Users access Fabrication Pro over the public internet using any modern browser. All connections are HTTPS-only with TLS 1.3 enforced. No plain HTTP connections are permitted. Application code runs in the user's browser as standard HTML/CSS/JavaScript — no plugins, no agents, and no sensitive processing client-side.

Zone 2 — Edge Security (Cloudflare)

Cloudflare sits at the perimeter of Fabrication Pro's entire infrastructure. It is the first point of contact for all inbound traffic and provides independently certified security controls before any request reaches Fabrication Pro's servers.

WAF	Filters OWASP Top 10 attack patterns, injection attempts, and malformed requests

DDoS protection	Automatic traffic scrubbing at scale — Fabrication Pro remains available during volumetric attacks
TLS termination	TLS 1.3 enforced at the edge; origin connections use re-encrypted HTTPS
CDN	Static assets cached globally for performance; dynamic requests proxied to origin
Compliance	Cloudflare holds FedRAMP Moderate, SOC 2, ISO 27001, and PCI DSS Level 1 certifications

Zone 3 — Fabrication Pro Application Layer

The Fabrication Pro application layer handles authenticated requests, enforces workspace RBAC, manages the development and publishing workflow, and coordinates all reads and writes to the underlying infrastructure. This layer is stateless with respect to your data — all state lives in GitHub (your code) and AWS (your data). Fabrication Pro can be replaced or migrated without any data loss.

Zone 4 — Source Code Layer (GitHub)

All application code generated and managed by Fabrication Pro is stored in a GitHub repository owned by your organization. This is not a Fabrication Pro repository — it is yours. If you disconnect from Fabrication Pro, your code remains fully accessible in your GitHub account and can be built and deployed using any standard development toolchain.

Your Code Belongs to You

Fabrication Pro uses the GitHub App model (not OAuth) for fine-grained, repository-scoped access. When you connect GitHub, you choose whether to grant access to selected repositories or all repositories — we strongly recommend selected repositories only. Your code, your commit history, and your CI/CD pipeline remain entirely within your GitHub organization.

Zone 5 — Data & Infrastructure (AWS via Supabase)

Fabrication Pro's data layer is built on AWS — specifically via Supabase, a managed Backend-as-a-Service that operates across 17 AWS regions globally and runs exclusively on AWS Graviton processors. This is the same infrastructure tier used by companies like Mozilla, 1Password, and GitHub.

Database	PostgreSQL on AWS EC2 Graviton. Standard, open-source, portable. Full schema export available at any time for migration
Authentication	Supabase GoTrue: email, OAuth providers, SSO (SAML/OIDC), MFA, and PKCE. HIBP compromised-password check available
Storage	Amazon S3: server-side AES-256 encryption, bucket-level IAM policies,

	S3-compatible API
Edge Functions	Deno on AWS compute: serverless, no persistent state, region-constrained
Data residency	EU, US, or AU region selected at account provisioning. Data does not leave the selected region by default
AWS regions (EU)	eu-west-1 (Ireland), eu-west-2 (London), eu-central-1 (Frankfurt)
AWS regions (US)	us-east-1 (N. Virginia), us-west-1 (N. California)
AWS regions (AU)	ap-southeast-2 (Sydney)

Zone 6 — Cross-Cutting Services

Two services operate across all other zones: Google Cloud KMS (Zone 2 key management, described above in the Encryption section) and the AI Inference Gateway. The AI gateway routes requests to a pool of foundation model providers, all of which are contractually prohibited from using your data to train their models.

Compliance & Certifications

SOC 2 Type II	ISO 27001:2022	GDPR	EU AI Act	FedRAMP
Prepared	Prepared	DPA Available	Low Risk	Path Defined-Prepared

If our client decides to move forward with Fabrication Pro or a similar solution, the architecture we have designed and built the platform upon can achieve the two most rigorous third-party security certifications commonly pursued by enterprise organizations: SOC 2 Type II and ISO/IEC 27001:2022.

SOC 2 Type II validates that security controls are not only properly designed but have also operated effectively over an extended observation period. ISO/IEC 27001:2022 certifies that the organization maintains a comprehensive Information Security Management System (ISMS) aligned with internationally recognized security standards and operational governance practices.

While Fabrication Pro is currently a proof of concept (POC), it is a highly comprehensive and enterprise-oriented POC built upon our extensive experience architecting and delivering secure, scalable enterprise solutions. Every layer of the platform has been

intentionally designed with these certification objectives in mind. Achieving these certifications would require additional operational maturity, formal governance processes, auditing, and ongoing investment, all of which have been considered within the long-term architectural strategy and roadmap for the platform.

Compliance Summary by Framework

GDPR (EU)	Data Processing Agreement available. DPO appointed (dpo@fabricationpro.com). EU data residency option. Data subject rights (access, deletion, portability) supported. 72-hour breach notification commitment. Standard Contractual Clauses for transfers
CCPA / CPRA (California)	'Do Not Sell or Share' opt-out mechanism. Data subject rights (access, deletion, portability). Data minimization commitments in DPA
UK GDPR / DPA 2018	DPA covers UK data subjects. UK-adequate transfer mechanisms in place
PIPEDA (Canada)	Consent, access, and correction rights supported. Data minimization commitments
Privacy Act 1988 (AU)	AU data residency available. Australian Privacy Principles (APPs) alignment
NIST SP 800-53	SOC 2 and ISO 27001 controls map to NIST 800-53 Rev 5 security control families. Full mapping available for FedRAMP ATO package preparation
HIPAA	NOT supported. The Fabrication Pro platform must not be used to process, store, or transmit Protected Health Information (PHI). Healthcare workloads require a separate HIPAA-authorized deployment

GovCloud Readiness

Fabrication Pro is on a defined path to FedRAMP authorization and GovCloud deployment. The underlying technology stack is entirely composed of components that have established GovCloud equivalents. No architectural redesign is required — GovCloud deployment is a migration of the existing stack into FedRAMP-authorized regions and services.

GovCloud Status — Planned, Not Yet Active

The GovCloud deployment described in this section represents Fabrication Pro's roadmap, not its current state. Clients with active FedRAMP, IL4, IL5, or ITAR requirements should contact the Fabrication Pro Enterprise team to discuss current availability and timelines before deployment.

Migration Path by Zone

Zone	Current	GovCloud Target
Zone 2 — Cloudflare	FedRAMP Moderate	Cloudflare for Government (FedRAMP Moderate authorized). FedRAMP High: confirm with Enterprise team
Zone 3 — App Layer	Commercial cloud	Containerized deployment to AWS GovCloud (US) ECS/EKS. No architectural changes required
Zone 4 — GitHub	github.com (Azure)	GitHub Enterprise Cloud – US Government (FedRAMP Moderate). IL4/IL5: GitLab Federal or self-hosted option
Zone 5 — AWS/Supabase	17 commercial regions	Deploy to AWS GovCloud (US-East / US-West). FedRAMP High authorized. Direct Supabase GovCloud deployment path
Zone 6 — GCP KMS	Google Cloud commercial	Migrate to AWS KMS CMK in GovCloud (FIPS 140-2 Level 2). Eliminates cross-cloud key dependency
Zone 6 — AI Gateway	Multi-provider commercial	Constrain to AWS Bedrock GovCloud only. Anthropic Claude available via Bedrock GovCloud for IL2. Higher IL levels: dedicated VPC model deployment

Impact Level Alignment

IL2 — Controlled Unclassified	Current commercial stack is suitable with FIPS 140-2 encryption enabled and FedRAMP-authorized IdP. AWS Bedrock GovCloud available for AI inference. GitHub.com FedRAMP Moderate covers source code
IL4 — CUI Sensitive	Requires full migration to AWS GovCloud (US). GitHub Enterprise US Government required. AI inference limited to AWS Bedrock GovCloud. All personnel with environment access must meet USG requirements
IL5 — National Security	Requires dedicated GovCloud tenant isolation. Self-hosted Supabase on dedicated EC2 instances. AWS KMS Customer Managed Keys. No shared multi-tenant infrastructure. On-premises or isolated VPC model deployment for AI inference
ITAR	All data processing must remain within US borders. AWS GovCloud (US) regions. GitHub Enterprise US Gov. No cross-cloud key management (eliminate GCP KMS). AI inference to US GovCloud endpoints only

Shared Responsibility Model

Security on Fabrication Pro is a shared responsibility between the platform, its infrastructure providers, and you as the client. Understanding where each party's responsibility begins and ends is essential for maintaining a secure deployment.

Layer	Fabrication Pro Responsibility	Your Responsibility
Platform security	SOC 2 Type II and ISO 27001 controls; security scanning pipeline; RBAC enforcement; secrets encryption; WAF; incident response	Configuring SSO/MFA at your identity provider; granting least-privilege roles to your users; reviewing and acting on Security Center findings
Source code	GitHub App integration with repository-scoped permissions; commit attribution; audit logs	Restricting GitHub App to selected repositories only; protecting main branch with PR reviews; rotating secrets when notified
Database access	RLS enforcement at PostgreSQL layer; automated RLS scanning pre-publish; schema-level security checks	Writing correct RLS policies; independently validating RLS effectiveness; not storing prohibited data (PHI, government IDs, etc.)
Data residency	Enforcing selected region at infrastructure layer; not moving data cross-region by default	Selecting the correct region at account provisioning; confirming with the Enterprise team for regulated workloads
Compliance	Platform-level SOC 2, ISO 27001, GDPR DPA, and subprocessor chain	Executing the DPA before processing personal data; maintaining your own compliance program; not uploading data Fabrication Pro is not authorized to process

Recommended Security Configuration

Identity & Access

- Configure SSO with SAML or OIDC — supported providers include Okta, Microsoft Azure AD, and Google Workspace
- Enable SCIM for automated user provisioning and deprovisioning
- Enforce MFA at your identity provider level — Fabrication Pro does not bypass MFA
- Apply least-privilege RBAC: assign editing and publishing as separate roles, not a combined permission
- Restrict GitHub App to selected repositories only when connecting Fabrication Pro to your

GitHub organization

Data & Compliance

- Select your required data residency region (EU / US / AU) at account provisioning — this cannot be changed without a full migration
- Execute the Fabrication Pro Data Processing Agreement before processing any personal data
- Do not upload Protected Health Information (HIPAA), government identifiers, or financial account numbers — these are contractually prohibited
- Document Fabrication Pro in your organization's Records of Processing Activities (ROPA) if operating under GDPR

Application Security

- Run a full four-scanner security review before every production publish
- Independently validate RLS policy effectiveness in Supabase using policy simulation tools — do not rely on scanner presence-check alone
- Resolve all high-severity scanner findings before publishing; document accepted risks for medium findings
- Use the Conversational Security Review for any application that handles sensitive business data
- For enterprise deployments: obtain an AI penetration test report through the Fabrication Pro AI Pentest feature

Credentials & Secrets

- Store all API keys and credentials in the Fabrication Pro encrypted secrets store — never hardcode in source files or prompts
- Rotate all secrets on a 90-day cycle or immediately following any security event
- If your organization has any projects built before November 2025, rotate all credentials in those projects now

Contact & Support

Security concerns	security@fabricationpro.dev — for security questions, vulnerability reports, and incident response
Privacy & DPA	privacy@fabricationpro.dev — DPA execution, data subject rights, GDPR inquiries

Enterprise & GovCloud	enterprise@fabricationpro.dev — GovCloud readiness, FedRAMP ATO preparation, IL4/IL5 deployments
Trust Center	trust.fabricationpro.dev — SOC 2 Type II report (NDA required), ISO 27001 certificate, subprocessor list
Vulnerability disclosure	Managed via HackerOne — email disclosure@fabricationpro.dev for submission instructions
Incident notification	Fabrication Pro will notify affected clients within 72 hours of confirming any notifiable data breach

Disclaimer

This document reflects Fabrication Pro's security architecture and commitments as of May 2026. Security postures evolve over time. Clients should verify current certification status and platform capabilities directly with the Fabrication Pro team before making compliance or procurement decisions. This document does not constitute legal or compliance advice and does not substitute for a 3PAO-certified FedRAMP assessment.