ReguShield AI
PILOT SUCCESS KIT

PILOT DOCUMENTATION

Security Whitepaper

Part of the ReguShield AI Pilot Success Kit — everything your team needs to run a successful compliance-intelligence pilot.

This document describes ReguShield AI's pilot environment as currently implemented. It is provided for customer due diligence and is not a warranty or certification.

---

1. Purpose

This whitepaper gives prospective customers' security and compliance teams an accurate picture of how ReguShield AI's pilot environment is built, how customer data is isolated and protected, and where our security programme is mature versus still on the roadmap. We document our posture honestly and do not claim certifications we do not yet hold.

---

2. Architecture Overview

ReguShield AI is a compliance decision-support application built on:

- **Application layer:** Next.js (App Router) / React, deployed on Vercel with automatic TLS.
- **Database & auth:** PostgreSQL via Supabase, hosted in the **European Union** (Dublin / Amsterdam region).
- **Authentication:** Supabase Auth (email/password) with session token management.
- **Storage:** Supabase Storage for evidence and document uploads.

All case data, analysis logs and audit records are stored **within the European Union**. Cloud (Supabase) is the authoritative source of truth for all customer data; the browser holds only a transient cache (see Section 8).

---

3. Tenant Isolation

Tenant isolation is enforced at the database layer, not just in application code.

- **Email-keyed workspaces.** Every workspace and every `pilot_*` table row is keyed by the **verified Supabase session email**. One email maps to one isolated workspace.
- **Postgres Row-Level Security (RLS).** Every `pilot_*` table carries RLS policies that check `auth.jwt() ->> 'email'` against the row's owner. A user can only read or write rows that belong to their own verified email.
- **Fail-closed by design.** If the email claim is absent from the JWT for any reason, the policies **deny access** — they never fail open. Access is denied rather than leaked.
- **Storage isolation.** Storage objects are organised into per-user folders keyed by email, protected by the same RLS model, so uploaded evidence and documents are scoped to the owning workspace.

For multi-member organisations, an active member is resolved to their workspace owner's email before any read or write, so invited teammates share one workspace by design rather than seeing across organisations.

---

4. Encryption

- **At rest:** AES-256 encryption via the Supabase managed database.
- **In transit:** TLS for all API and web traffic between the client, the application and Supabase.

Application secrets (database credentials, API keys) are held in Vercel environment variables and are never exposed in the client bundle.

---

5. Audit Trail

ReguShield AI maintains **application-level** audit trails that record:

- Data uploads and ingestion batches
- Remediation and compliance actions
- Evidence submissions and lifecycle changes
- Report generation events

These are application logs written by the platform, timestamped and tied to case/workspace references. They are **not** Postgres-level database triggers; they are intended to give compliance teams an in-app activity record, not a tamper-proof database-engine audit log.

Report integrity. Exported reports carry a content hash, a signature block and an audit envelope so a recipient can verify a report has not been altered after generation.

---

6. Access Control

- **Invite-only pilot access.** Pilot workspaces are not open to self-service signup. Access is granted by invitation / admin approval.
- **Single-use activation.** Activation links are **single-use** and **expire after 7 days**.
- **Session tokens.** Supabase Auth issues and manages session tokens; authenticated state is the basis for all RLS checks above.

---

7. Client Cache & Purge Behaviour

To provide instant load, the browser keeps a local cache (`localStorage`) of workspace state. This cache is a convenience layer only — **Supabase remains the RLS-protected source of truth.** The cache:

- Is **purged on logout**.
- Is **purged on inactivity timeout**.
- Is **replaced when a different user signs in on the same device** (owner-change purge), so one user's cached data is not exposed to another account on a shared machine.

No compliance decision relies on the local cache; if it is lost or cleared, state is rehydrated from Supabase under that user's RLS scope.

---

8. Dependency Security

- `npm audit` runs on dependency updates.
- Critical and high-severity CVEs are patched before deployment.

An internal review against the OWASP Top 10 has been completed. An external, full-scope penetration test is planned (roadmap — not yet completed).

---

9. Backups & Disaster Recovery

Backups rely on **Supabase's managed backup capability** for the EU-hosted PostgreSQL database. We do not operate a separate backup pipeline.

Honest limitation: we do not publish a verified Recovery Point Objective (RPO) or Recovery Time Objective (RTO) for the pilot environment, because recovery characteristics are a function of the managed platform and we will not state figures we cannot independently guarantee. A formal disaster-recovery runbook is in preparation (roadmap).

---

10. Incident Handling

Incident handling for the pilot is **best-effort**:

- We monitor application and deployment logs for errors and anomalies.
- On becoming aware of a security incident affecting customer data, we will **investigate, contain, and notify affected customers** at the contact on file, together with the information available to us at that time.

Honest limitation: we do **not** operate a formal 24/7 Security Operations Centre (SOC), and we do **not** commit to a specific incident-response SLA or notification timeframe for the pilot. A formalised incident-response process with defined timelines is on the roadmap. Where a legal notification obligation applies (e.g. a personal-data breach under GDPR), we will act in line with that obligation as data processor and support the customer as controller.

---

11. Certifications Status

We are deliberately precise here so no claim is overstated:

STANDARD	STATUS
ISO/IEC 27001	**Not certified.** Internal gap assessment against ISO 27001:2022 Annex A controls completed; controls implementation and external certification are on the roadmap.
SOC 2	**Not held.** No SOC 2 Type I or Type II report exists at this time; scoping is on the roadmap.
External penetration test	Not yet completed; planned (roadmap).

No representation is made that ReguShield AI holds ISO 27001, SOC 2 or any equivalent certification today.

12. Current Limitations / Roadmap

So that nothing in this document is read as more than it is, the following are **not** in place today:

- No ISO 27001 certification (gap assessment done; certification on roadmap).
- No SOC 2 report (on roadmap).
- No completed external penetration test (planned).
- No published RPO/RTO; backups rely on the managed platform.
- No formal 24/7 SOC; incident handling is best-effort with customer notification.
- Audit trails are application-level logs, not database-engine triggers.
- EU GDPR representative identified; formal appointment planned for Q3 2026.

These items are tracked and will be updated as the programme matures.

13. Security Contact

For security questions, vulnerability reports or due-diligence requests:

hello@regushield.ai