VAULTPASS · SECURITY DOCUMENTATION

Internal Security Self-Assessment

Date: 14 June 2026

Type: Grey-box source review (internal self-assessment)

Scope: Next.js web application — cryptographic core, authentication, all API routes, succession / heir-release protocol, HTTP security headers & CSP

Method: Manual source review and dependency / secret scan, modelled on Cure53 methodology. No live exploitation.

> **This is an internal self-assessment, not an independent third-party audit.** It documents our own pre-engagement review conducted by the core team. An independent external audit by a specialist security firm is scheduled for H2 2026; its full report will be published on completion. This document is provided for transparency about our internal process.

1. Scope & Coverage

AREA	REVIEWED
Client-side cryptography (AES-256-GCM, Shamir's Secret Sharing)	✓
Server-side shard encryption	✓
Authentication, MFA, and password reset	✓
Vault API and encrypted import	✓
Succession / heir-release and Dead-Man's-Switch logic	✓
Payments and inbound webhooks	✓
HTTP security headers and Content-Security-Policy	✓
Secret scanning across the full repository	✓

2. Findings Summary

No Critical or High findings. The zero-knowledge model holds: secrets are AES-256-GCM encrypted client-side, the key is split via Shamir's Secret Sharing before anything is stored, and the server never receives plaintext or the full key.

A small number of **Medium** findings identified during the review cycle were **remediated prior to publication** — covering authentication step-up on destructive actions, generic error responses to prevent

information disclosure, and fail-closed rate limiting on sensitive endpoints. Remaining items are **Low / Informational** hardening recommendations, tracked internally and included in the scope handed to the external auditor.

> Detailed finding identifiers, reproduction steps, and the residual hardening backlog are withheld from this public document by design — they will be addressed and verified during the external engagement. We do not publish a live map of internal hardening items.

3. Cryptographic Verdict

- **Vault encryption:** AES-256-GCM with a fresh 256-bit key per secret and a fresh random 96-bit IV per encryption; the GCM authentication tag is retained. No IV reuse; integrity is protected.
- **Server shard encryption:** a per-(user, node-type) key derived via HMAC-SHA-256 over a high-entropy server secret, with a random IV and stored authentication tag.
- **Shamir's Secret Sharing (GF(256)):** correct multiplicative inverse, consistent reduction polynomial, 2-of-3 threshold, coefficients drawn from a CSPRNG — information-theoretic secrecy holds below the threshold.

Residual cryptographic items are all Low / Informational. The core is sound enough to hand to an external auditor with confidence.

4. Reporting Security Issues

Responsible-disclosure contact: `support@vaultpass.network` (subject line “Responsible Disclosure”). Machine-readable policy: `/.well-known/security.txt` (RFC 9116). Programme details: `vaultpass.network/security/bug-bounty`.
