Security Overview

Trust & assurance pack for procurement reviewers - last updated 2026-05-09

WIAG handles sensitive estate, identity and document data for South African families and the practitioners who serve them. The summary below is written for procurement, risk and information-security reviewers performing vendor due diligence on WIAG.

Penetration testing

WIAG commissions an external penetration test on an annual cadence, with a focused re-test after any major release that changes authentication, payments, file storage or the LifeKey death-trigger workflow. Findings are tracked to remediation in our internal task system; high or critical findings block the next release until fixed or a documented compensating control is in place.

Most recent test window: April 2026 (annual external test). The next scheduled test window is April 2027.

Compliance posture and roadmap

Today

- Registered Financial Services Provider (FSP No. 55699) regulated by the FSCA.
- POPIA-aligned processing under a published Privacy Policy and Information Officer (Natalie Macdonald Spence, privacy@wheniamgone.co.za).
- Internal controls baseline: documented threat model, STRIDE walkthrough, controls map, security requirements and risk register, refreshed on every security-relevant release.
- PAIA manual published. Coordinated Vulnerability Disclosure policy published at /responsible-disclosure with safe-harbour wording and triage SLAs.

Roadmap (targets, not current state)

Q4 2026	Complete SOC 2 Type I readiness assessment and remediation backlog.
Q2 2027	Achieve SOC 2 Type I attestation.
Q4 2027	Begin SOC 2 Type II observation window.
Q2 2028	Achieve SOC 2 Type II attestation; evaluate ISO 27001 certification path.

Roadmap items are stated as targets, not as a current state. Where a target slips, this page is updated and the new quarter is published before the original deadline passes.

Continuous monitoring, SAST and dependency scanning

Static application security testing (SAST). Runs on every change, plus a full scheduled sweep before each release. Triaged by the security owner; high/critical findings block release.

Dependency / supply-chain scanning. Runs on every change against the lockfile and on a daily schedule against published advisories. Triaged by the security owner; CVEs with a working production exploit path are patched within 7 days.

Runtime application monitoring. Always on. Tamper-alert windows, audit-chain integrity checks, suspicious access patterns and PDF queue health are monitored continuously. Pages on-call when an alert fires; weekly review of low-severity signals.

Threat-model refresh. Re-walked on every security-relevant change (new external integration, new auth surface, new admin route, new file-upload flow, key rotation, security-advisory dependency upgrade, or launch milestone). Owned by the security owner; new e15-score risks are escalated to the WIAG owner before the change ships.

Coordinated vulnerability disclosure

Researchers can report security issues to security@wheniamgone.co.za under the published policy at /responsible-disclosure. We acknowledge reports within two business days, confirm severity and remediation timeline within ten business days, and credit the researcher in our hall of thanks once the issue is resolved (with their permission). Safe-harbour wording protects good-faith research conducted within scope.

Data-handling summary

- Consumer vault entries (assets, debts, contacts, instructions) are encrypted in the user's browser using a key derived from their passphrase, before leaving the device.
- Uploaded vault documents are encrypted in the user's browser; only ciphertext and an integrity hash are stored.
- Authorised sharing workflows use server-side envelope encryption so professionals can be granted scoped, audited access without holding the consumer's passphrase.
- Payment card data never touches WIAG infrastructure - it is handled by Paystack; we hold only references and last-four digits.
- All state-changing operations write to an append-only audit log with hash-chained tip witnesses.

Procurement contact

For vendor questionnaires, security questionnaires (SIG / CAIQ), data-processing addenda, or to request the latest pen-test summary letter under NDA, contact security@wheniamgone.co.za with the subject line "Procurement". We aim to return completed questionnaires within ten business days.