HAVEN AID
— MAKING AN IMPACT —

072 601 1647 061 382 5253
info@havenaid.org www.haveaid.org
Remote
"A Safe Haven for Everyone, Everywhere."

Haven Connect Integration Security Whitepaper

How Haven Connect Protects Data During External Synchronisation
Version 3.0 — April 2026

1. Executive Summary

Haven Connects Integration Gateway is designed to enable secure, compliant, and controlled collaboration between government systems and partner organisations.

This whitepaper provides a comprehensive overview of the security mechanisms that protect sensitive data throughout every integration lifecycle event.

Haven Connect is built on three core principles:

- **Security by Design** — Protection is embedded at every layer
- **Privacy by Default** — Only minimal, necessary data is ever shared
- **Full Accountability** — Every action is logged, traceable, and auditable

2. Security Architecture Overview

Haven Connect uses a **multi-layered defence-in-depth architecture** to ensure data remains protected at all times.

Security Layers

1. Authentication & Identity
2. Transport Encryption
3. Request Integrity Validation
4. Data Minimisation Controls
5. Audit & Monitoring Systems

Each layer operates independently and collectively to mitigate risk.

3. Authentication & Identity Management

All integrations are secured using organisation-scoped API keys.

Key Characteristics

- 256-bit cryptographically secure key generation
- Secure storage using SHA-256 hashing
- One-time visibility upon creation
- Scoped permissions (read, write, sync)
- Configurable rate limiting

Additional Controls

- API key revocation at any time
- Optional IP whitelisting for trusted environments
- Key rotation policies for long-term security

4. Transport Security

All data transmitted between Haven Connect and external systems is encrypted in transit.

Standards Enforced

- **TLS 1.3 encryption (mandatory)**
- Rejection of insecure protocols (TLS 1.0, 1.1, SSLv3)
- Certificate pinning recommended for high-trust integrations

This ensures protection against interception and unauthorised access.

5. Request Integrity & Anti-Tampering Controls

To ensure every request is authentic and unmodified:

Mechanisms

- HMAC-SHA256 request signing
- Timestamp validation (5-minute window)
- Replay attack prevention

Outcome

- Prevents request forgery
- Blocks replay attacks
- Guarantees message integrity

6. Data Minimisation & Privacy Controls

Haven Connect strictly enforces **data minimisation** in accordance with POPIA.

Data Protection Rules

- No session transcripts or clinical notes are transmitted
- Personally identifiable information is anonymised
- Only explicitly approved data fields are shared
- Field-level control per integration connection

Transparency

Each synchronisation event records exactly:

- What data was shared
- When it was shared
- Which system initiated the request

7. Role-Based Access Control (RBAC)

Access to integration features is restricted using a strict role hierarchy.

Role	Permissions
Organisation Admin	Full control over integrations, API keys, and data configuration
Manager	Read-only access to integrations and logs
Supervisor	Read-only access to logs
Professional	No access to integration features

This ensures separation of duties and minimises insider risk.

8. Audit Logging & Monitoring

All integration activity is logged in an **immutable audit trail**.

Logged Data Includes

- Sync type and direction
- Timestamp of execution
- Data fields transmitted
- Initiating user or system
- Execution duration
- Success or failure status
- Error details (if applicable)

Retention Policy

- Logs retained for **7 years**
- Fully exportable for audits and investigations
- Compliant with South African regulatory requirements

9. Threat Model & Risk Mitigation

Haven Connect proactively identifies and mitigates key security threats.

Threat	Mitigation Strategy
Stolen API Key	Immediate revocation, IP whitelisting, scoped permissions, rate limiting
Man-in-the-Middle Attack	TLS 1.3 encryption, HMAC signatures, certificate pinning
Data Overexposure	Data minimisation, field-level controls
Replay Attacks	Timestamp validation and request signing
Insider Threats	RBAC, audit logs, enforced key rotation
External System Breach	Limited exposure due to anonymised and minimal data sharing

10. Incident Response Framework

Haven Connect follows a structured and compliant incident response process.

Immediate Actions

- Revoke all affected API keys
- Suspend compromised integrations
- Preserve audit logs for investigation

Notification Protocol

- Notify affected organisations within **72 hours** (POPIA requirement)
- Provide detailed incident reports where necessary

Regulatory Cooperation

- Audit logs available to the Information Regulator
- Full traceability of events ensured

11. Compliance & Regulatory Alignment

Haven Connect is aligned with leading global and South African standards.

Frameworks Supported

- **POPIA** — Protection of Personal Information Act (South Africa)
- **GDPR** — General Data Protection Regulation
- **ISO/IEC 27001** — Information Security Management
- **Children's Act 38 of 2005** — Protection of minors' data

12. Security Best Practices for Partners

To maintain a secure integration environment, all partners should:

- Store API keys securely (never expose in frontend code)
- Implement IP whitelisting where possible
- Use certificate pinning for sensitive systems
- Rotate API keys regularly
- Monitor logs for suspicious activity
- Implement retry logic with exponential backoff

13. Conclusion

Haven Connect delivers enterprise-grade security for all external integrations.

Through layered protection, strict access controls, comprehensive auditing, and strong regulatory alignment, the platform ensures that sensitive data remains protected at every stage of the integration lifecycle.

14. Contact & Support

For security reviews, integration support, or compliance inquiries:

- Website: **www.havenaid.org**
- Team: Haven Connect Security Team