HEDRON
ANALYTICS

Tensor Technical Security Data Sheet

Security and confidentiality are foundational principles for Tensor, and the following precautions and measures are implemented for all deployments. This data sheet is current as at January 2026 and additional enhancements may have been made since publication.

Authentication & Access Control

- **Two-Factor Authentication (2FA):** Enforced across both development environments and end-user access for all administrators and user managers. Can be enabled across an organization if requested by the customer.
- **Role-Based Permissions:** User access is restricted to the logged-in user and identified organization managers. Tensor system administrators may read and edit user information **via the user management system (currently Auth0[1])** with appropriate authorization and user permission. Tensor system administrators do not store user personally identifiable information (PII) within the application. Tensor admin credentials are issued on a controlled, limited basis.
- **Credential Segregation:** Distinct credentials are maintained for each system, and system administrators must maintain separate credentials for admin and user accounts.

Session & Communication Security

- **Ephemeral Session Tokens:** All communication between third-party services (e.g., commercial avatars) and backend agents is secured with short-lived tokens, minimizing repeated credential handling and reducing the risk of replay attacks. No PII (e.g., name, email) is intentionally shared with third-party services by the system. User inputs that contain PII are user-provided content and outside of Hedron's control. These may be processed or stored by third-party providers if submitted.
- **Encrypted Transport:** All traffic between the frontend, backend, and third-party providers (e.g., Anam, Decis API, GCP services) is secured using TLS 1.2+ encryption.
- **Scoped API Keys:** Provider integrations (e.g. Anam, Groq, Decis, etc.) require scoped API credentials stored securely in environment variables or platform secret management and are never exposed in code repositories.
  - **Note:** Hedron is aggressively localizing services to reduce exposure to and use of third-party APIs in Tensor to improve efficiency and residue dependencies.

Infrastructure & Compliance

- **Cloud Hosting on Certified Providers:** Development and deployment environments run exclusively on services compliant with SOC 2 and ISO/IEC 27001 standards (currently Google Cloud).

[1] Auth0 - https://auth0.com/

- **Environment Isolation:** Separate environments for development, staging (live testing), and production prevent cross-contamination and ensure configuration isolation.
- **Secrets Management:** All sensitive keys and credentials are injected at runtime via environment variables or platform secret management; .env files are excluded from version control.
- **Secure Password Management:** Keeper[2] password manager is used for secure, auditable storage of passwords with role-based shared vaults to ensure backup access while limiting exposure.
- **Data at Rest:** Data stored within Google Cloud services is encrypted at rest by default[3] using provider-managed encryption.

Monitoring & Operational Security

- **Audit Logging:** Administrative and system audit logs track access events, session metadata, and operational activity but do not contain PII or conversation content. User conversation logs are stored in customer-controlled Google Cloud Storage buckets and may contain conversation data; these logs are not part of routine administrative workflows. Users are identified in audit logs only by pseudonymous user IDs managed in a separate system.
- **Least-Privilege Principle:** Administrative credentials and system permissions are tightly scoped, minimizing the attack surface.
- **Code Backups:** GitHub and local backups are maintained. In future production services, automated backup and recovery systems will ensure fallback coverage if a primary provider becomes unavailable. PII and credentials are not included in GitHub backups. Local backups are encrypted.

Future Security Enhancements

- **Compliance Alignment:** Data retention and storage practices are designed to align with client-specific compliance requirements (e.g., GDPR, HIPAA where applicable). Work to comply with DoD IL5 is ongoing and scheduled to be complete by end of Q1 2026.
- **Client Data Control:** Application data is logically separated per customer and stored in dedicated or compartmentalized storage under customer control rather than embedded in the application itself. From level 2.5 onward (see level definitions below), all data storage and retention are fully customer managed.
- **Resilience & Disaster Recovery:** Production deployments will incorporate backup services, ensuring continuity in the event of primary provider outages.

[2] Keeper Security - https://www.keepersecurity.com/
[3] Google Cloud Security: Data at Rest - https://docs.cloud.google.com/docs/security/encryption/default-encryption

Deployment Configurations

Based on these security guidelines, Tensor deployments fall into one of the following general categories based on the user’s needs and requirements.

- **Level 1 — Hedron-hosted (pseudonymous):**
  Hedron Analytics hosts the application and identity service. The application stores and logs only system-generated pseudonymous user and organization IDs. PII is held exclusively in the identity provider and accessed only transiently for user interface display or authorized administrative actions, fetched directly from the identity system, and never persisted or logged by the application. Customer data is stored in logically separated storage buckets rather than within the application itself.
- **Level 2 — Customer-managed identity, Hedron storage (anonymous to Hedron):**
  Hedron hosts the application and data storage, while authentication and user management are handled by the customer’s identity system. Hedron receives only opaque user and organization identifiers and does not have access to user PII.
- **Level 2.5 — Customer-managed identity and storage (Hedron hosted, customer managed):**
  Hedron hosts the application framework, but authentication, identity management, data storage, and logging are provided and controlled by the customer. The application accesses customer storage during active sessions and maintains only ephemeral in-memory state, which is cleared at session termination. Hedron retains only anonymized operational session metadata.
- **Level 3 — Fully customer-hosted:**
  The application, authentication, identity management, storage, and logging run entirely within the customer’s environment. Hedron does not process or access user identity or application data at any stage.

Please contact the Hedron CTO with any specific questions or to request an updated data sheet.

Andrew Sheves: andrew@hedronanalytics.com