**Security & Privacy Requirements Documentation**

*Outlining encryption, authentication, data governance, and consent frameworks*

**Key Frameworks:**

* **GDPR** (for EU-hosted data)
* **UN Personal Data Protection and Privacy Principles**
* **ISO 27001 / 27018**
* **National Data Protection Acts** (e.g., Kenya’s Data Protection Act 2019)

**Security Requirements:**

| **Area** | **Requirement** |
| --- | --- |
| **Encryption** | AES-256 for data at rest; TLS 1.3 for data in transit |
| **Authentication** | OAuth 2.0 / OpenID Connect; Biometric or MFA for mobile users |
| **Role-Based Access Control (RBAC)** | Granular permissions tied to user roles (e.g., Field Officer, HR Analyst) |
| **Audit Logs** | Immutable logs for all data views, edits, exports |
| **Secure Hosting** | Encrypted cloud storage in approved UN/NGO-compliant regions |

**Privacy & Consent:**

* **Consent Forms** (multi-language, digital + paper fallback)
* **Data Minimization**: Only essential data collected for operational needs
* **Right to Access & Erasure**: Users can request review or deletion (with supervisor approval flow)
* **PII Segregation**: Personally identifiable information (e.g., phone, ID, health status) stored in secure vault table
* **Incident Response Plan**: Includes breach notification protocol within 72 hours