**Security & Privacy Requirements Documentation**

**Purpose:** To ensure systems are designed to protect sensitive data (e.g., personal health information, student records, farmer subsidies) in alignment with best practices and contextual risks.

**Key Inclusions:**

* **Encryption Standards:**
  + **Data-at-Rest**: AES-256 for stored files/databases
  + **Data-in-Transit**: TLS 1.3/SSL for secure connections (HTTPS, SFTP)
* **Authentication & Identity Management:**
  + Multi-factor authentication (MFA) for staff/admins
  + OAuth 2.0 / OpenID Connect for partner system access
  + Role-based access controls (RBAC) or attribute-based access control (ABAC)
* **Access Control Matrix:**
  + Maps system users → roles → access rights (e.g., view/edit/delete permissions)
  + Includes internal users, field agents, and external stakeholders
* **Audit Logs & Monitoring:**
  + Track data access, login attempts, changes, and export events
  + Integration with SIEM tools if applicable
* **Data Minimization & Retention:**
  + Store only necessary PII
  + Define how long data is retained, then archived or anonymized
* **Vulnerability & Threat Modeling:**
  + Identify risks such as man-in-the-middle attacks, SQL injection, device theft
  + Include mitigation strategies like firewalls, secure boot, device-level encryption