Swarga Foundation: Data Protection Policy

Effective Date: January 12, 2026

Approved By: J. Swarnalatha, Managing Trustee

1. Core Principles

- **Lawfulness & Consent:** Personal data (beneficiary, donor, staff) is collected only with explicit consent and for legitimate foundation purposes.
- **Data Minimization:** Only information essential for the Foundation's programs is collected and stored.
- **Purpose Limitation:** Data will not be used for any activity beyond what was agreed upon at the time of collection.

2. Storage Protocols

A. Physical Storage (External Hard Drives)

- **Device Encryption:** All Foundation hard drives must use system-level encryption to prevent unauthorized access if the device is lost or stolen.
- **Physical Security:** When not in use, hard drives must be stored in a locked safe or cabinet within the Foundation's office.
- **Inventory Management:** The **Director of Programs** maintains a log of all physical storage devices, including who is currently in possession of each.
- **Prohibited Use:** Staff are not permitted to use personal hard drives or USB sticks for Foundation data.

B. Cloud Storage (Google Workspace / Cloud Services)

- **Managed Systems:** Digital records must be kept in approved, managed information systems (e.g., Google Drive) rather than unsynchronized desktop locations.
- **Encryption in Transit & Rest:** Cloud providers must be vetted to ensure they use industry-standard encryption (TLS/HTTPS) for data moving to and from the cloud and for data stored on their servers.
- **Multi-Factor Authentication (MFA):** Mandatory MFA must be enabled for all cloud accounts to add a layer of security beyond passwords.

3. Access & Security Measures

- **Least Privilege Access:** Access to sensitive folders (e.g., medical records of beneficiaries) is restricted to specifically authorized personnel based on their role.
- **Password Integrity:** Staff must use strong, unique passwords and are prohibited from sharing credentials or writing them down in visible areas.

4. Data Retention and Disposal

- **Retention Period:**
    - **Financial Records:** Retained for 7 years as per legal requirements.
    - **Beneficiary Data:** Retained while the individual is active in Foundation programs and for 3 years thereafter.
- **Secure Disposal: * Digital:** Files must be "wiped" using secure deletion software rather than just moved to the trash.
    - **Physical:** Damaged or decommissioned hard drives must be physically destroyed to ensure data is irretrievable.

5. Monitoring and Review

In accordance with the **Swarga Foundation's Monitoring and Review Process**:

- **Quarterly Self-Review:** The committee will audit access logs and storage inventory to ensure compliance.
- **Annual Data Audit:** A comprehensive review of all stored data will be conducted to identify and delete obsolete records.
- **Breach Notification:** In the event of a data breach (e.g., a lost hard drive), the **Managing Trustee** and affected individuals must be notified within 72 hours.