SISTRY FOUNDATION

Management Information System (MIS) Policy

1. Introduction & Purpose

Since its inception in 2009, SISTRY FOUNDATION has been dedicated to driving impactful social change. To support its growing operations, ensure transparency, and maintain data integrity, this **Management Information System (MIS) Policy** establishes a structured framework for data collection, processing, reporting, and security.

The purpose of this policy is to streamline decision-making, optimize stakeholder reporting, and protect the sensitive data of beneficiaries, donors, and staff.

2. Scope

This policy establishes a universal standard of accountability that spans all levels of the SISTRY FOUNDATION hierarchy. It applies unconditionally to full-time and part-time employees managing day-to-day operations, grassroots volunteers inputting field data, and specialized consultants advising on organizational strategy. By explicitly binding board members to these regulations, the foundation ensures that leadership sets a compliance example from the top down. This collective oversight guarantees that anyone representing the foundation maintains the same high standards of data integrity.

The technical scope of this policy covers every digital and physical information system owned, leased, or utilized by the foundation. This includes core infrastructure such as centralized cloud databases, donor management software, and financial accounting portals, as well as the hardware used to access them, such as office desktops, field-level mobile data collection devices, and official email accounts.

This policy governs the lifecycle of all data assets generated or held by the foundation since its inception. This includes sensitive beneficiary personally identifiable information (PII), confidential financial records, grant proposals, and strategic internal metrics. The scope dictates that whether data is being actively collected in the field, processed for a quarterly report, or archived for historical tracking, it must be handled with the highest level of confidentiality and compliance, treating data as a core institutional asset.

3. Core Objectives of the MIS

- **Data Integrity:** For an NGO with nearly two decades of fieldwork, trust is built on accurate data. This objective ensures that data—whether it is a financial transaction, a field survey, or a beneficiary profile—remains consistent and error-free throughout its lifecycle. By moving to real-time updates, the MIS eliminates the risks of outdated information or duplicated efforts, ensuring that what is visible on the management dashboard matches the reality on the ground.

Registered Office: Prangopal Nagar,
P.O. - Nabadwip, Nadia, Pin-741302

SARATHI COMPLEX, Room No.102,
Vill: Suluntu ,P.O.-Parulia (Purbasthali-II),
Dist.-Purba Bardhaman, Pin-713513

Phone: 03454-296103/9332047221
e-mail: sistry09@gmail.com Website: www.sistryindia.org

- **Evidence-Based Decisions:** SISTRY FOUNDATION shifts from intuitive decision-making to data-driven strategy. The MIS acts as a centralized engine that transforms raw field data into actionable analytics. By tracking program metrics over time, leadership can objectively evaluate which initiatives are yielding the highest social return on investment. This allows management to confidently allocate scarce resources, scale successful projects, and pivot away from ineffective strategies.
- **Accountability & Compliance:** Operating transparently is essential for maintaining relationships with institutional donors, regulatory bodies, and auditors. The MIS streamlines this by automating the generation of structured, tamper-proof reports. Whether satisfying statutory requirements, fulfilling tax-exempt compliance, or providing granular utilization reports to international donors, the system ensures that SISTRY FOUNDATION can quickly and accurately prove exactly where and how every unit of funding was utilized.
- **Data Security:** Safeguarding information is both a legal requirement and an ethical duty, especially when handling sensitive beneficiary data. This objective focuses on establishing a digital fortress around the foundation's assets. By implementing strict encryption, access controls, and threat monitoring, the MIS actively defends against data breaches, identity theft, and cyberattacks. Protecting this data preserves the dignity and safety of the communities SISTRY FOUNDATION serves.

4. System Architecture & Data Governance

4.1 Data Categorization

To ensure appropriate handling and protection, SISTRY FOUNDATION categorizes its information based on sensitivity and the potential impact of exposure:

- **Public Data:** This information is intentionally prepared for the public eye to showcase the foundation's impact and maintain transparency. It includes audited annual reports, participant success stories, and fundraising materials. Because it poses zero risk to the organization, it is open for unrestricted distribution across websites, social media, and press releases.
- **Internal Data:** This consists of institutional knowledge required for day-to-day operations, such as Standard Operating Procedures (SOPs), project workflows, and internal communications. While not harmful if minor details leak, unauthorized exposure can disrupt operational efficiency. Access is limited to internal staff and active volunteers.
- **Confidential Data:** This is the most sensitive layer of information, encompassing beneficiary Personal Identifiable Information (PII), financial bank ledgers, donor records, and HR files. Unauthorized access could lead to legal liabilities, financial fraud, or a breach of trust with vulnerable communities. This data requires strict encryption and role-based access.

4.2 Data Collection & Entry Protocols

- To eliminate transcription mistakes caused by transferring paper notes to computers, field staff must input data directly at the source using secure mobile applications or web portals. Standardized drop-down menus, checkboxes, and mandatory fields minimize human entry

errors and enforce data uniformity from day one.

- Every action within the MIS leaves a digital footprint. The system automatically attaches metadata—including the exact date, timestamp, and unique user login credentials—to every new entry or modification. This ensures complete accountability and allows system administrators to trace the origin of any data discrepancy.
- Data accuracy requires continuous verification. Every week, designated Project Heads must compare a sample of the digital system entries against physical field realities or secondary receipts. This process catches anomalies early, flags training gaps among field staff, and guarantees that leadership acts on verified information.

5. Access Control & Security Measures

5.1 Role-Based Access Control (RBAC)

Access to the MIS is strictly governed by the principle of least privilege. Users are granted access only to the data necessary to perform their specific job functions.

User Role	Access Level	Permitted Actions
Field Staff / Volunteers	Restricted	Data entry for assigned projects; view-only for local beneficiary lists.
Project Managers	Moderate	Edit/Approve project data; generate regional performance reports.
Finance & HR Team	Specialized	Full access to financial ledgers, payroll, and donor databases.
Executive Leadership	Global	View-only access to organization-wide dashboards; approval of structural changes.
IT Administrator	System	Technical configuration, backup management, and user provisioning (no data editing rights).

5.2 Password & Authentication Policy

- A secure system relies heavily on the strength of its individual access points. Requiring a minimum of 12 characters—combining uppercase and lowercase letters, numbers, and special symbols—drastically reduces the vulnerability to automated "brute-force" hacking attempts. This baseline standard ensures that weak, easily guessable choices (such as "Sistry2009" or "Password123") cannot be used, creating a strong first line of defense for the entire network.
- As field teams and remote consultants frequently access the MIS outside the primary office network, passwords alone are no longer sufficient. Multi-Factor Authentication (MFA) acts as a vital secondary lock. Even if an attacker manages to steal a user's password, they cannot gain access without a secondary, time-sensitive verification code sent directly to the employee's authorized mobile device or authenticator app. This significantly mitigates the risk of unauthorized external intrusions.

- **90-Day Lifecycle:** Regularly changing passwords limits the window of opportunity for an undetected, compromised credential to be exploited by bad actors.
- **No Account Sharing:** Every user must operate via their own unique account. Prohibiting shared logins ensures strict individual accountability, making it possible to accurately trace exactly who viewed, edited, or deleted specific data within the system logs during an audit.

6. Data Backup & Disaster Recovery (DR)

To prevent data loss due to hardware failure, cyberattacks, or natural disasters, SISTRY FOUNDATION enforces the following backup protocol:

- **Automated Backups:** To minimize human error or forgetfulness, backups are fully automated through system scripts.
  Daily Incremental Backups: The system identifies and copies only the data that has changed or been newly created since the previous day. This saves bandwidth and storage space while capturing daily fieldwork.
  Weekly Full Backups: Every week, the system clones the entire database. This layered approach ensures that if a server fails, the foundation loses less than 24 hours of operational progress.
- **Offsite Redundancy:** Storing all backups with a single cloud provider creates a single point of failure; if that provider experiences a massive outage or a ransomware attack compromises the main account, all data could be lost. By maintaining a monthly backup in an isolated, secondary cloud environment managed under separate credentials, SISTRY FOUNDATION creates a digital firewall. If the primary system is completely compromised, the organization can rebuild from this clean, independent fallback image.
- **Testing:** A backup strategy is only as good as its ability to restore data when things go wrong. Files can occasionally become corrupted during the backup process without throwing immediate errors. Requiring the IT Administrator to conduct a simulated data recovery drill twice a year guarantees that the files are actually readable and that the team knows exactly how to bring systems back online under pressure, minimizing downtime during a real emergency.

7. Compliance & Ethical Data Use

- **Beneficiary Consent:** As an NGO, SISTRY FOUNDATION interacts with individuals who may be in vulnerable situations. Obtaining informed consent means clearly explaining to beneficiaries—in a language they understand—what data is being collected, why it is needed, and how it will be used. Securing this digitally (via checkboxes/signature pads) or in writing *before* data entry ensures the foundation respects individual autonomy and establishes a legally sound foundation for data processing.
- **Anonymization:** While sharing success stories and impact metrics is vital for fundraising and donor engagement, it must never compromise a beneficiary's safety. Anonymization involves stripping away or altering direct identifiers—such as changing real names, obscuring

specific village locations, or using generalized age ranges. This allows the foundation to showcase its meaningful work and satisfy donor reporting requirements without exposing individuals to social stigma or privacy risks.

- **Regulatory Alignment:** SISTRY FOUNDATION must continuously align its MIS infrastructure with evolving legal landscapes. This includes adhering to national data privacy laws (such as the Digital Personal Data Protection Act) regarding how citizen data is handled. Additionally, the system must precisely track and categorize funds to comply with strict NGO financial regulations, foreign contribution laws, and standard tax-exemption audits, ensuring the foundation safeguards its legal status and operational license.

8. Policy Violations & Review

8.1 Enforcement: Maintaining Accountability and Consequences

A policy is only effective if it is actively enforced. This point establishes a zero-tolerance stance toward behaviors that compromise SISTRY FOUNDATION's security or reputation.

- **Types of Violations:** It clearly defines infractions, ranging from careless actions (like leaving a logged-in device unattended or neglecting password safety) to severe misconduct (such as intentionally leaking confidential donor databases or falsifying field metrics).
- **Disciplinary Matrix:** To ensure fairness and legality, consequences are progressive and scaled to the severity of the breach. Minor oversights may result in mandatory retraining or formal warnings, while severe or malicious violations trigger immediate termination of employment or contracts, alongside civil or criminal legal proceedings to recover damages.

8.2 Review Cycle

A static policy quickly becomes obsolete in a rapidly shifting digital and regulatory environment. By mandating an annual review, SISTRY FOUNDATION guarantees its protocols remain dynamic and relevant.

- **Technological Advancements:** As new cyber threats emerge and better data tools become available, the MIS framework must adapt to integrate stronger security features.
- **Changing Regulatory Requirements:** Data privacy and NGO compliance laws frequently shift. Annual evaluations ensure the foundation always operates within the latest legal frameworks, preventing costly penalties.
- **Organizational Growth:** As the foundation scales—adding more field projects, employees, and data volume—the policy is continually updated to support expanding operational needs without compromising security.

Approved By:
Executive Director,
SISTRY FOUNDATION
Date of Adoption: May 19, 2026

TARUN KUMAR RAY
Digitally signed by TARUN KUMAR RAY
Date: 2026.05.19 16:54:44 +05'30'