INFORMATION SECURITY POLICY MANUAL

8	Asset	An asset is anything that has value to the organization. Assets can be classified into the following 5 categories: 1. Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) 2. Physical assets: (computer equipment, communications, utility equipment, buildings etc.) 3. Software assets: (database information, applications, software code, development tools, operational software etc.) 4. People assets: UIDAI human resources and stakeholders. 5. Service assets: (Logistics, building management systems, communications, utilities etc.)

1. Introduction: JEEVAN REKHA

The Government of Kerala disburses social security pensions to eligible citizens under various categories, such as old age, disability,widow pensions and welfare fund board pension . To continue receiving their benefits, pensioners are required to muster annually.With advancements in information technology and the integration of Aadhaar, biometric verification has made identity authentication more efficient and reliable. This service allows pensioners to verify their identity using Aadhaar-based biometric authentication.The system facilitates pensioners to complete their biometric authentication at Akshaya Kendras operated through KSITM under Government of Kerala. This ensures a streamlined, transparent, and secure process, enhancing the integrity of the pension disbursement system.

FINANCE DEPARTMENT shall ensure the confidentiality, integrity, and availability of these at all times by deploying suitable controls commensurate with the asset value and in accordance with applicable rules.

Confidentiality: No critical data / information shall be disclosed to any person within or outside the department, other than persons who are authorized to use that data.

Integrity: No critical data / information or programs shall be allowed to be modified by anyone without proper authority and authorizations. This will ensure safeguarding the accuracy and completeness of information and processing methods. No critical data shall be modified, added, edited or deleted except by users or programs that are authorized to do so and, in a manner, as approved or designated.

Availability: All Information Systems including hardware, communication networks, software Programs and the data contained therewith shall be made available only to authorized users at any time solely for carrying out their assigned responsibilities.

Information Security Management System (ISMS) describes the basic security measures, which include internal computer systems and information stored on them, information processing systems that are used for research and analysis, data stored in the Data server of State Data center as well as printed material.

Document Objective

The objective of this document is to lay down the structure of the security organization

3. Objectives

The objective of this Information Security Policy is to establish a structured approach to managing information risks and to provide directives for the protection of information assets across the Jeevan Rekha , FINANCE DEPARTMENT and third-party service providers. This policy ensures the confidentiality, integrity, and availability of Jeevan Rekha ,FINANCE DEPARTMENT's information assets, including Aadhaar-related data, in compliance with the Aadhaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, 2016 (Central Act 18 of 2016) , UIDAI regulations, and applicable standards.

4. Ownership

Finance department is the ultimate owner of this policy and is responsible for information security at the strategic level.

5. Responsibility

- To maintain segregation of duties and avoid conflict of interest:
  - The Information Risk Management Team (IRMT) within the department is the custodian of the Information Security (IS) Policy and oversee its formulation, periodic review, and maintenance.
  - Implementation and compliance with the policy shall be the responsibility of the IT Security Team, functioning under the IT Division.
- The Chief Information Security Officer (CISO) is responsible for:
  - Articulating and coordinating the Information Security Policy for the protection of information assets.
  - Addressing security-related concerns within the organization and liaising with relevant external agencies such as UIDAI.
  - The CISO shall function independently of the IT Department to maintain neutrality and shall report directly to the Risk Management Division or its

promptly under the guidance of the CISO .

9. Information Security Governance

Information Security Governance is an integral framework of leadership, organizational structures, and processes that ensure the protection of Jeevan Rekha, FINANCE DEPARTMENT's information assets and mitigation of evolving security threats.

- **Critical Outcomes of Information Security Governance:**

  - **Strategic Alignment**

    Ensure information security strategies are aligned with departmental goals to support key objectives, including compliance with UIDAI regulations and other legal requirements.

  - **Risk Management**

    Identify, assess, and mitigate risks to reduce the potential impact of threats to acceptable levels.

  - **Performance Measurement**

Monitor and evaluate the effectiveness of information security through defined metrics and regular reporting to ensure organizational objectives are met.

  - **Optimized Investment**

    Balance and prioritize investments in information security measures to maximize support for departmental objectives.

- **Organizational Necessities and Benefits:**
  - Increased Predictability: Reducing uncertainty in operational activities.
  - Decision Assurance: Ensuring decisions are based on reliable and secure information.
  - Enhanced Risk Management: Strengthening the ability to identify and address

10. Various service providers rendering services to FINANCE DEPARTMENT are as follows:

SPARK PMU, FINANCE DEPARTMENT		
Sr.	**Services**	**Service Providers**
1	Data Centre Infrastructure Provider and maintenance	KSDC
2	Backbone Link in KSDC	NKN, BSNL and Sify
3	Internet Link in FINANCE DEPARTMENT	KSWAN
4	Electricity Provider	Kerala State Electricity Board(KSEB)
5	Telephone Provider	BSNL
6	Water	KWA

10.1. Roles and Responsibilities

The roles and responsibilities of the Information Security Organization members are defined to ensure effective implementation and governance of the Information Security Management System (ISMS).

❖ **Chief Information Security Officer (CISO)**

- Establish, implement, monitor, and continually improve the Information Security Management System (ISMS).
  - Periodically review information security policies and procedures, recommending improvements to align with emerging risks and regulations.
  - Coordinate ISC meetings and provide consultative inputs on security requirements.
- Lead and oversee departmental information security initiatives, ensuring compliance with policies and regulations.
  - Regularly update the ISC on information security programs, issues, and incidents.

FINANCE DEPARTMENT's Information Security Policy.

- Provide security architecture for IT systems and infrastructure.
- Monitor the operational effectiveness of mandatory IT controls.

- Analyze internal and external security incidents, identify lessons learned, and propose measures for future prevention.

❖ **Technology Infrastructure Service Providers**

Strategic outsourced partners manage and operate infrastructure services on behalf of Jeevan Rekha, FINANCE DEPARTMENT under Service Level Agreements (SLAs).

Key Responsibilities:

- Implement and operate the IT infrastructure in compliance with Jeevan Rekha, FINANCE DEPARTMENT's Confidentiality, Integrity, and Availability requirements.
- Develop and maintain Standard Operating Procedures (SOPs) and Security Guidelines for managed assets.
  - Ensure IT asset management aligns with Jeevan Rekha, FINANCE DEPARTMENT's approved policies and procedures.
- Provide timely reports on infrastructure performance and compliance with security standards.

❖ **End Users**

End Users include Akshaya centres who interact with Jeevan Rekha, FINANCE DEPARTMENT's information systems and assets.

Key Responsibilities:

- Account Usage: Use their assigned accounts, devices, and removable media responsibly and in alignment with information security policies.
- Password Management: Safeguard the confidentiality of passwords, ensuring they are not shared or stored insecurely and will be responsible for any breaches through their respective credentials.
- Information Protection: Protect sensitive and business-critical information from unauthorized access, modification, or destruction.
- Incident Reporting: Report any known or suspected security incidents, including potential breaches or suspicious activity, immediately to their User Manager or the IT Security team.
- Policy Adherence: Stay informed and comply with all information security policies, procedures, and training provided by FINANCE DEPARTMENT.

11. Policies, Procedures, and Guidelines

Finance Department considering the security and compliance requirements, Information Security policies has been framed based on a series of security principles. These principles ensure robust protection of information assets, particularly Aadhaar-related data, and compliance with standards like ISO27001, ISO27701, NIST Cybersecurity Framework, and the Aadhaar Act.

Below are the key policies and their purposes:

scheme will be implemented for all data processed or stored by Jeevan Rekha. The level of security provided to information will directly correlate with its classification.

- **Classification Levels:** Data shall be classified into categories such as Confidential, Restricted, and Public based on the sensitivity of the information, such as Aadhaar data, and related information.
- **Security Measures:** Each classification level will have specific security controls, including access restrictions and encryption, to ensure that sensitive information is adequately protected.

11.4. Access Control Policy

Access to information is granted based on the principle of least privilege, ensuring that only authorized personnel can access specific data. The policy ensures the need to protect sensitive information (e.g., Aadhaar-related data) with the need to provide access to those who require it for legitimate business purposes.

- **Granularity of Access:** Access levels are defined for different roles (surveyors, administrative staff, external partners) to ensure that individuals can only access data necessary for their work.
- **Authentication**: Strong authentication methods will be implemented to validate access requests.

11.5. Email Security Policy

The Finance Department will implement systems and procedures to ensure that emails are used efficiently for business communication and to prevent misuse.

- **Secure Email Operations:** The email system must be secure for internal communication as well as for communication with external stakeholders, such as Government agencies or contractors, ensuring that sensitive data is not exposed or misused.

- **Security Requirements:** Secure development practices will be adopted, including regular code reviews, testing for vulnerabilities, and application security audits.

11.9. Network Security Policy

To ensure the protection of data both within the department's networks and over public networks, security measures are implemented to protect systems from unauthorized access and data leakage.

- **Access Controls:** Firewalls, intrusion detection systems (IDS), and encryption are deployed to safeguard sensitive data..
- **Network Monitoring:** The department's networks are monitored continuously for suspicious activities, with immediate actions taken to mitigate any potential threats.

11.10. Anti-Virus | Firewall Policy

KSDC using antivirus and anti-malware solutions to protect systems from malicious software that could compromise the security of sensitive information.

- **Malware Protection:** Anti-virus software will be installed on all endpoints, to detect and prevent the spread of malware.
- **Regular Updates:** All systems will be updated regularly with the latest security patches to defend against new threats.

11.11. Backup & Recovery Policy

To safeguard against data loss due to hardware failure, natural disasters, or other unforeseen events, NIC will implement automated backup and recovery procedures.

- Regular vulnerability assessments and penetration testing are conducted to identify and mitigate potential risks.
- Data at rest and in transit, especially Aadhaar and survey data, is encrypted using strong algorithms to prevent interception or unauthorized access.

Organizational Measures:

- A comprehensive Information Security Management System (ISMS) governs data security practices, ensuring accountability at all levels.

- Incident response teams are established to handle breaches swiftly and minimize impact.

11.14. Aadhaar Data Security

- The Aadhaar number is collected over a secure application, transmitted through secure channels as per UIDAI specifications, and any identity information returned by UIDAI shall be securely stored.
- Biometric information is not collected by FINANCE DEPARTMENT. Aadhaar authentication is conducted using OTP-based authentication only.
- OTP information shall be collected through a secure application, encrypted on the client device, and transmitted over secure channels in accordance with UIDAI specifications.
- Aadhaar number is not retained. The entity shall only retain the parameters received in response from UIDAI, ensuring compliance with privacy and security guidelines.
- e-KYC information shall be stored exclusively in encrypted form, meeting UIDAI encryption standards and adhering to the latest industry best practices.
- FINANCE DEPARTMENT does not store Aadhaar numbers of

    - Records of Aadhaar holders' consent for authentication.
    - Note: PID information shall not be retained under any circumstances.
- An Information Security Policy aligned with the ISO 27001 standard, UIDAI- specific Information Security Policy, and the Aadhaar Act, 2016, shall be formulated and implemented to ensure the security of identity information.
- Aadhaar numbers, if stored, shall only be stored in the Aadhaar Data Vault as per UIDAI specifications.

11.15. Database Security Procedure

In compliance with the Information Security Policy, all databases owned and managed by the department are secured to uphold their confidentiality, integrity, and availability.

Key Procedures:

- **Access Management:** Database access is restricted to authorized personnel based on the principle of least privilege. All access is logged and monitored.
- **Database Encryption**: Sensitive fields, including personally identifiable information (PII) and Aadhaar data, are encrypted at the database level.
- **Audit Trails:** Database activities are logged and reviewed periodically to detect and prevent unauthorized actions.
- **Backup and Recovery:** Regular backups are taken and stored securely to ensure data recovery in case of system failures.
- **Patch Management**: Databases are kept up to date with the latest security patches to protect against vulnerabilities.
- **Database Classification:** Databases are classified based on the sensitivity of the data they store Specific security controls are applied accordingly.

❖ **Compliance with Information Security Policy and Procedures**

Use of Information Processing Facilities:

All are required to use information processing facilities in alignment with the Information Security Policy and Acceptable Usage Policy.

Monitoring and Privacy:

- The department respects the privacy of its personnel; however, it reserves the right to monitor and audit the use of its systems and data.

- Monitoring includes the review of emails, application logs, and activities on devices owned or managed by the department to ensure security.

Policy Exceptions:

- Deviations from the Information Security Policy or Procedures must be approved through the Exception Management Process.
  - Exceptions are reviewed annually or as necessary based on emerging threats and risks.

Disciplinary Measures:

Any violations or attempts to breach security policies or procedures will result in disciplinary actions.