INFORMATION SECURITY POLICY MANUAL

DOCUMENT CONTROL INFORMATION

Document ID	**:**	**Information Security Policy Manual**
Classification	**:**	**Public**
Issue Date	**:**	**17/02/2025**

Distribution List			
Name	**Position/ Role**	**Author/Approver/ Reviewer/ For Information**	**Organization**
Akhil S	Sr.Hardware Support Engineer	Author	DSLR
Vincent A Ferrer	GIS Expert	Reviewer	DSLR
Salim S	Deputy Director (SPMU)/CISO	Reviewer	DSLR
Bhavana S. Bhasi	Law Officer	Reviewer	DSLR
Sri. Aji Kumar B	Administrative Officer	Reviewer	DSLR
Seeram Sambasiva Rao IAS	Survey Director	Approver	DSLR

Change History					
Version No	**Page No**	**Details of Change**	**Approved Date**	**Reviewed By**	**Approved By**
1	All	Initial document	07/02/2025		Seeram Sambasiva Rao IAS

Table of Content

Terms and Definitions

S. No	Terms	Definition
1	AAS	AADHAAR Authentication Server
2	API	Application Program Interface
3	AUA/ASA	Authentication User Agency/Authentication Service Agency
4	Sub-AUA	Sub Authentication User Agency
5	CA	Certifying Authority
6	CIDR	Central Identities Data Repository
7	CN	Common Name
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.)

9	Information /Information Asset (IA)	Information that has value to the organization (UIDAI). Including but not limited to Citizen biometric and demographic information, personally identifiable information, employee information,organization information such as CIDR details etc.
10	IT	Information Technology
11	KUA	Know your customer User Agency
12	NDA	Non-Disclosure Agreement
13	NTP	Network Time Protocol
14	OTP	One Time Password
15	PID	Personal Id entity Data
16	SOP	Standard Operating Procedures
17	SPOC	Single Point of Contact
18	SSL	Secure Sockets Layer
19	STQC	Standard Testing and Quality Control
20	VA	Vulnerability Assessment
21	VPN	Virtual Private Network

1. Introduction: Directorate of Survey and Land Records

In the realm of sustainable land administration, up-to-date cadastral data is essential for managing land tenure, ownership, valuation, and use. Kerala has been at the forefront of evolving its Land Administration System (LAS) since 1905, yet separate textual and spatial records have historically limited the ability to reflect current land transactions and real-time updates. To address these challenges, the Kerala Government launched the **Digital Resurvey Mission** under the 'Ente Bhoomi' initiative, re-engineering the Land Administrative System (LAS) into a comprehensive, citizen-centered **Integrated Land Information Management System (ILIMS)**. This digitally managed system spans 1,550 villages, leveraging advanced geospatial technology such as Real-Time Kinematic (RTK) GNSS Rovers, a Continuously Operating Reference Stations (CORS) network, and Robotic Electronic Total Stations (R-ETS) for high-precision surveys thus establishing a reliable geospatially integrated land record database with each parcel tagged by a Unique Land Parcel Identification Number (ULPIN), or Bhu-Aadhar.

At the heart of 'Ente Bhoomi,' the Integrated Portal unifies land-related services from the Revenue, Registration, and Survey Departments, a first of its kind online webgis portal for efficient land governance. Accessible through a Single Sign-On (SSO) portal, citizens can seamlessly avail all land related services online especially , initiate template-based land registration, and benefit from automatic land record mutations without visiting multiple government offices. Following the official launch of ILIMS in October 2024 the Ente bhoomi system is set to scale rapidly, transforming service delivery and citizen engagement across Kerala. Moreover, Ente bhoomi enables Aadhaar integration in LPM in an attempt to provide high level services for citizens. Aadhaar integration in LPM also supports revenue administration, land-use planning, environmental conservation, and land dispute resolution.

Therefore, Security of UIDAI Information Assets handled by the DSLR for providing services, is of paramount importance. DSLR 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 all employees shall follow to protect the department's information assets, 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 centre as well as printed material.

Document Objective

The objective of this document is to lay down the structure of the security organization in DSLR, for governing ISMS along with a set of policies and procedures that need to be implemented and followed to ensure that the information assets of DSLR remain secure, available, confidential and in a state where it would be reliable and accurate.

2. Scope

- This policy applies to all employees, contractors, partners, interns/trainees working within the Department of Survey and Land Records (DSLR). Third-party service providers, such as the State Data Center (SDC) for hosting services ,National Informatics Center (NIC) for application development, and any other relevant departments are also required to comply with this policy.
- The scope of this Information Security Policy includes all information stored, communicated, and processed within DSLR, as well as any departmental data handled or hosted by third-party service providers or external entities.
- This Information Security Policy applies to all instances where Aadhaar-related information is processed and/or stored by DSLR, or associated third parties. The policy ensures adherence to the Aadhaar Act, 2016, UIDAI regulations, and industry-leading standards such as ISO 27001, NIST Cybersecurity Framework, and ISO 27701.
- This policy shall be reviewed periodically and may be amended in accordance with the evolving legal, regulatory, and operational requirements set forth by UIDAI or other relevant authorities.

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 all units of the Department of Survey and Land Records (DSLR) and third-party service providers. This policy ensures the confidentiality, integrity, and availability of DSLR’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

The Director of the Department of Survey and Land Records 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 equivalent.
- ❖ All employees, contractors, and third-party service providers, including those from SDC and NIC, are responsible for upholding the confidentiality, integrity, and availability of the department’s information assets as outlined in this policy.

6. Policy Exceptions

Policy exceptions shall be addressed through a defined Exception Handling Procedure, ensuring that all deviations are documented, justified, approved, and periodically reviewed by the Information Risk Management Team (IRMT) in consultation with the CISO.

7. Periodic Review

- ❖ This policy shall undergo a comprehensive review annually or whenever significant changes occur in the existing IT environment, processes, or regulatory framework that may affect its scope and procedures.

- The Chief Information Security Officer (CISO) is responsible for conducting the review and recommending necessary updates.
- The updated policy shall be submitted to the Director (DSLR) for review and final approval.
- This policy will remain in effect until the next scheduled review or revision.

8. Policy Compliance Check

- A compliance review of the Information Security Policy will be conducted periodically by Internal or External Auditors to ensure adherence to the policy.
- The Inspection and Audit Division (IAD) will oversee compliance monitoring and prepare a comprehensive compliance report.
- This report will be presented to the Audit Committee of DSLR for evaluation and action.
- Non-compliance findings will be documented, and remedial actions will be initiated promptly under the guidance of the CISO and the Inspection and Audit Division.

9. Information Security Governance

Information Security Governance is an integral framework of leadership, organizational structures, and processes that ensure the protection of DSLR'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 risks effectively.
  - Legal Protection: Minimizing exposure to legal liabilities related to information security breaches.
  - Process Improvements: Streamlining procedures for greater efficiency and effectiveness.
  - Loss Prevention: Mitigating financial and reputational losses from security-related incidents.
  - Reputation Management: Enhancing trust and credibility among stakeholders, including citizens and partnering agencies.

10. Organizational Structure of DSLR

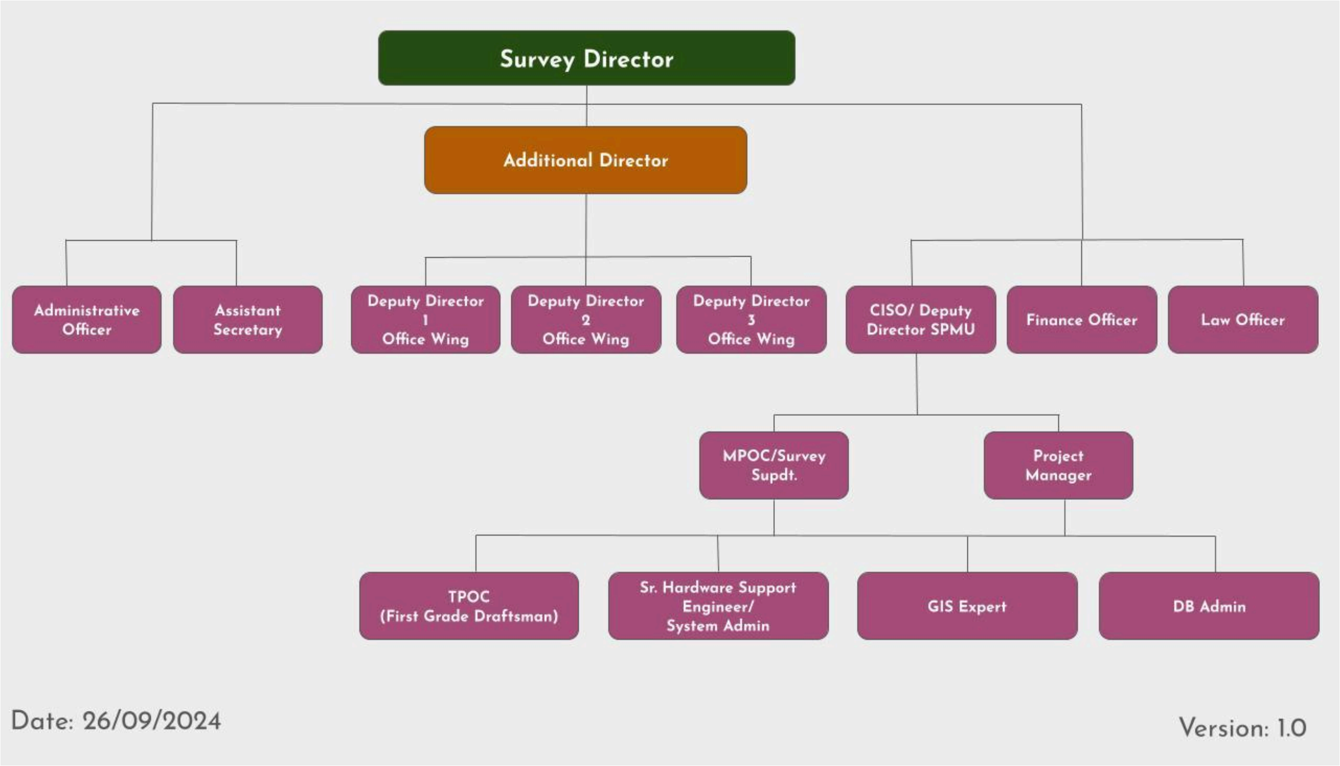
Survey Director
Additional Director
Administrative Officer
Assistant Secretary
Deputy Director 1 Office Wing
Deputy Director 2 Office Wing
Deputy Director 3 Office Wing
CISO/ Deputy Director SPMU
Finance Officer
Law Officer
MPOC/Survey Supdt.
Project Manager
TPOC (First Grade Draftsman)
Sr. Hardware Support Engineer/ System Admin
GIS Expert
DB Admin
Date: 26/09/2024
Version: 1.0

Table 1:

Role	Name, Designation, Contact No.
CISO	Shri.Salim S , Deputy Director,SPMU, DSLR; 0471 232 5266
DISO – HR	Aji Kumar B, Administrative Officer, DSLR; 0471 232 5266
DISO – System Admin	Akhil S, Sr.Hardware Support Engineer,SPMU, DSLR; 0471 232 5266
ISMS – Internal Auditor	Internal audit team
ISMS - Consultant	Internal audit team

Various service providers rendering services to DSLR are as follows:
Table 2:

DSLR		
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 DSLR	BSNL,KFON,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).

- ❖ **Survey Director**
  - ➢ Approve the Information Security Policy and all associated sub-policies.
  - ➢ Oversee the governance and strategic alignment of information security initiatives with departmental goals.
- ❖ **Information Security Committee (ISC)**

The Chief Information Security Officer (CISO) shall serve as the Chairperson of the ISC. The committee will include representatives from the following:

- Chief Information Security Officer (CISO)
- Administrative Officer
- Law officer
- Additional Members (as needed): Internal Audit, Human Resources, Legal, Finance, and other relevant departments based on the agenda.

- ❖ **Roles and Responsibilities of the ISC:**

- Develop and implement information security policies and procedures to mitigate identified risks in alignment with the department's risk tolerance.
- Approve and monitor major information security initiatives, including projects, budgets, and action plans.
- Oversee the development and implementation of a department-wide Information Security Management Program.
- Review security incidents, assessments, and monitoring activities.
- Evaluate the effectiveness of security awareness programs and propose enhancements.
- Assess emerging information security challenges and ensure readiness.
- Generate and evaluate performance metrics for security controls.

- Provide regular updates on information security activities to the Survey Director.
- Conduct quarterly ISC meetings and maintain Minutes of Meetings (MOM) records.

❖ 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.
- Conduct and facilitate risk assessments for information assets, recommending mitigation strategies.
- Promote information security awareness among employees, stakeholders, and third-party service providers.
- Act as the primary point of contact for all internal and external security audits.
- Review system compliance for ISMS

❖ Information Asset Owner

Information Asset Owners are assigned to each information asset and are responsible for ensuring the implementation and maintenance of security processes for these assets.

Key Responsibilities:

- Assign the initial classification to information assets and periodically review the classification to ensure alignment with business needs under the guidance of the Information Risk Management Committee(IRMC).
- Implement and maintain recommended security controls for their respective assets as directed by IRMC.
- Regularly review and update access rights for the information assets they oversee.

- Define access criteria and backup requirements for the information assets or applications under their ownership.
- Retain overall responsibility for the security and compliance of the assets, even when delegating operational authority to an Asset Custodian.

❖ Asset Custodian

Asset Custodians are typically members of the Information Technology (IT) team and assist Information Asset Owners in securing and maintaining assets.

Key Responsibilities:

- Assist in identifying, developing, implementing, and maintaining security controls for assigned assets.
- Support the development of information asset inventories, ensuring Confidentiality, Integrity, and Availability (CIA) ratings are properly documented.
- Report any issues affecting information assets to the Asset Owner.
- Maintain operational controls and procedures under the guidance of Asset Owners while ensuring compliance with established policies.

❖ IT Security Team

The IT Security Team is responsible for executing the information security policies, frameworks, guidelines, and control processes to protect DSLR’s information assets.

Key Responsibilities:

- Enable and implement necessary information security controls.
- Develop IT security procedures and guidelines that align with DSLR’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 DSLR under Service Level Agreements (SLAs).

Key Responsibilities:

- Implement and operate the IT infrastructure in compliance with DSLR’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 DSLR’s approved policies and procedures.
- Provide timely reports on infrastructure performance and compliance with security standards.

❖ **Application Developers**

Application systems, including both business and generic software (e.g., middleware and databases), may be developed by internal teams or external third-party developers.

Key Responsibilities:

- Ensure systems are developed and maintained in adherence to DSLR’s information security requirements and policies.
- Incorporate user and security requirements during the development lifecycle.
- ❖ Collaborate with IT security to ensure risks in development and testing environments are mitigated.
- Regularly report to DSLR’s IT Security team on the status of applications and related security measures.

❖ **User Management Administrator**

The User Management Administrator is the immediate manager or supervisor responsible for overseeing the activities of employees, contractors, consultants, and other non-employee personnel under their supervision.

Key Responsibilities:

- Account Management: Ensure proper user account creation, maintenance, and deletion of user accounts for their team members, ensuring alignment with security policies.
- Asset Accountability: Maintain responsibility for all user IDs and information assets utilized by team members, including contractors and consultants.
- Activity Oversight: Monitor and ensure compliance with DSLR's security guidelines by all team members using DSLR’s information assets.
- Access Approval: Approve access requests to information systems and assets, ensuring access is granted based on necessity and job function.
- Incident Reporting: Promptly report any misuse or suspected violations of information security policies to the concerned authorities (e.g., IT Security or CISO).

❖ End Users

End Users include employees, contractors, consultants, and trainees who interact with DSLR’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 DSLR.

11. Policies, Procedures, and Guidelines

At the Department of Survey and Land Records, considering the security and compliance requirements, Information Security policies have 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:

11.1. Asset Management Policy

Information assets shall be identified, accounted for, and assigned a nominated asset owner. Owners shall:

- Be identified and cataloged for all information assets, including digital and physical records related to Aadhaar data and survey records.
- Be responsible for maintaining appropriate controls to safeguard the assets.
- Delegate specific control implementations to custodians as appropriate while retaining accountability for the overall protection of the assets.
- This policy ensures a structured approach to managing and protecting assets critical to the department's functions, in alignment with legal and regulatory requirements.

11.2. Information Risk Management Procedure

Detailed risk assessments for information assets (e.g., application risk assessment, infrastructure risk assessment) are undertaken to:

- Identify threats to information systems, including those storing Aadhaar data and other sensitive land records.
- Evaluate vulnerabilities and assess the likelihood and potential impact of such threats.
- Classify risks into acceptable, transferable, avoidable, or those requiring mitigation.
- Apply risk treatments through well-defined control mechanisms.
- The process will ensure compliance with ISO27001 (ISMS) and Aadhaar Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, 2016 (Central Act 18 of 2016) mandates while minimizing risks to the department's critical functions.

11.3. Data Classification Policy

To maintain the confidentiality, integrity, and availability of information, a data classification scheme will be implemented for all data processed or stored by the Department of Survey and Land Records. 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 land records, Aadhaar data, and related survey 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, land ownership records) 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 Department of Survey and Land Records 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.
- **Email Monitoring and Security Controls:** Policies to monitor email traffic and prevent phishing or unauthorized access are enforced.

11.6. Information Security (IS) Incident Management Policy

The incident management process is established to handle security breaches, ensuring quick responses and minimal impact on the department’s systems and data, particularly sensitive information like land records and Aadhaar data.

- **Incident Reporting:** All security incidents, including unauthorized access or data loss, are immediately reported to the Information Security Officer (ISO).
- **Incident Response:** Protocols are defined to assess, mitigate, and report security incidents, ensuring compliance with the Aadhaar Act and other regulatory requirements.

11.7. Change Management Policy

Changes to the department's IT systems, applications, and infrastructure are properly controlled to maintain system integrity and security. Any change in the systems storing sensitive data, such as land records, is ensured to follow a standardized procedure.

- **Change Control:** All changes to the systems are documented, tested, and authorized before being deployed to production environments.
- **Risk Assessment:** Each change will undergo a risk assessment to ensure it does not introduce vulnerabilities, especially in systems dealing with Aadhaar data.

11.8. Application Security Policy

All applications, including those used for managing survey and land records, will undergo security assessments and be developed following secure coding practices to safeguard against potential threats.

- **Security Requirements:** Secure development practices will be adopted, including regular code reviews, testing for vulnerabilities, and application security audits.
- **Third-Party Software:** Applications developed or maintained by third-party vendors must comply with departmental security standards and guidelines.

11.9. Network Security Policy

To ensure the protection of data both within the department's private 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, such as land records and Aadhaar details, during transmission.
- **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 Policy

The Department of Survey and Land Records will implement 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, including servers and employee workstations, 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, the Department of Survey and Land Records will implement automated backup and recovery procedures.

- **Data Backups:** All critical data, including survey records, land ownership information, and Aadhaar-related data, will be backed up on a scheduled basis.
- **Disaster Recovery:** Backup data are stored in geographically separated locations, and disaster recovery procedures will be in place to restore data in the event of a system failure.

11.12. Data Migration Policy

When migrating data from one system or database to another (e.g., during the upgrade of the department's land records system), the migration process must be carefully planned and executed.

- **Data Integrity:** Data integrity must be ensured during the migration process, and validation checks will be performed post-migration.
- **Sensitive Data Protection:** Any Aadhaar or personally identifiable information (PII) must be encrypted during the migration process to prevent unauthorized access.

11.13. Data Security

To ensure the confidentiality, integrity, and availability of sensitive information, including personal and Aadhaar-related data, the Department of Survey and Land Records adopts industry-standard physical, technical, and organizational measures. These measures are implemented in alignment with ISO27001, NIST Cyber Security Framework, and Aadhaar Act regulations.

Physical Security:

- Access to physical premises where sensitive information is processed or stored (e.g., data centers, document archives) is restricted to authorized personnel using access control mechanisms, such as biometric systems and key card authentication.
- Surveillance systems are deployed to monitor and record activities around secured areas.

Technical Security:

- Advanced security tools, including firewalls, intrusion detection systems (IDS), encryption mechanisms, and multi-factor authentication (MFA), are implemented to prevent unauthorized access to digital systems.
- 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.
- Regular security training and awareness programs are conducted for employees and contractors.
- 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 the Department of Survey and Land Records (DSLR). 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 or VID numbers submitted by residents or individuals to the requesting entity shall not be 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.
- DSLR does not store Aadhaar numbers of individuals or residents, ensuring their privacy and security in accordance with UIDAI's guidelines.
- As mandated by law, Aadhaar numbers and associated data is encrypted and stored only within a secure Aadhaar Data Vault (ADV) in compliance with UIDAI standards.
- All applications used for Aadhaar authentication or e-KYC shall undergo compliance testing with the Aadhaar Act, 2016, before deployment in production. Additionally, applications will be audited annually by UIDAI-recognized bodies such as STQC or CERT-IN.
- In the event of an identity information breach, the organization shall notify UIDAI within 72 hours, providing:
  - A description and consequences of the breach;
  - The number of Aadhaar holders and records affected/compromised;
  - Contact details of the CISO;
  - Mitigation measures taken.
- Appropriate security and confidentiality obligations shall be included in Non-Disclosure Agreements (NDAs) with employees, contractors, and other personnel handling identity information.
- Access to authentication applications, logs, servers, and sensitive infrastructure shall be restricted to authorized personnel. An access control list shall be maintained and regularly

updated.

- Best practices in data privacy and protection, based on international standards, shall be adopted to ensure security.
- Authentication transaction logs received from the Central Identities Data Repository (CIDR) shall be stored with the following details:
    - The Aadhaar number (or UID token for Local AUAs) against which authentication was sought;
    - Specified parameters from the authentication response;
    - Records of information disclosure to Aadhaar holders at the time of authentication;
    - 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 (e.g., Public, Restricted, Confidential). Specific security controls are applied accordingly.

11.16. Data Sanitization Guidelines

Data sanitization ensures that sensitive data in non-production environments, such as development and testing systems, is appropriately masked or obfuscated to protect it from unauthorized access.

Purpose:

To maintain the privacy of personal data and Aadhaar-related information while preserving the usability of data for testing and development purposes.

Sanitization Methods:

- **Masking**: Replace sensitive fields (e.g., Aadhaar numbers, personal identifiers) with dummy values.
- **Anonymization**: Transform data so that it is not linked to any individual while retaining its statistical utility.
- **Encryption**: Apply strong encryption to sensitive data that needs to remain visible only to authorized personnel.

Procedure:

- Identify sensitive fields requiring sanitization, including PII and Aadhaar-linked data.
- Apply sanitization during data migration to non-production environments.
- Verify the sanitization process through audits to ensure that no sensitive information remains exposed.
- By implementing robust data sanitization practices, the department ensures that privacy expectations are respected while maintaining the functionality of non-production systems.

11.17. Compliance

- ❖ **Compliance with Regulatory Requirements**

The Department ensures full compliance with all statutory, regulatory, and contractual obligations to safeguard information security and maintain operational integrity. Key measures include:

Legal Compliance:

- Adherence to Information Technology (IT) Act, 2000 and its amendments.
- Compliance with all directives, frameworks, and guidelines issued by regulatory authorities such as UIDAI and Aadhaar Act requirements.

Software and Intellectual Property:

Ensure compliance with licensing terms for proprietary software or other intellectual property in use. Maintain accurate records for the acquisition, renewal, and usage of software licenses.

Data Protection and Cross-Border Data Movement:

- Movement of sensitive data outside the country is subject to applicable data protection policy.
- The department will not share Aadhaar-related or personally identifiable information (PII) without proper authorization and encryption.

Records Management:

All records are retained, archived, and disposed off in line with legal, regulatory, and organizational retention schedules.

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

Use of Information Processing Facilities:

All employees, contractors, and partners 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, up to and including termination of employment or legal action.

❖ Information Systems Audit

Purpose of Audits:

Audits are conducted to ensure compliance with policies, identify gaps, and recommend improvements to information security practices.

Audit Control Measures:

- The use of information systems audit tools must be authorized by the CISO or a designated officer to prevent misuse.
- Strict logging and access control policies are to be enforced during audits to protect sensitive information.

Frequency and Reporting:

Audits are performed on a scheduled basis, as well as after significant changes in systems or policies.

Findings are reported to the relevant stakeholders, including the department head and governance committees, for necessary actions.

END OF DOCUMENT