

Data Protection and Security Guidelines for Registrars

1. Background

This document lays down the data protection and security guidelines to be followed by Registrars of the Unique Identification Authority of India (UIDAI). Since the Aadhaar enrolment process and the enrolment for the services of the Registrar is common, it is essential to define the parameters of responsibility of UIDAI and the Registrars.

There are two components to the enrolment process:

- a) **Enrolment for Aadhaar** – for which the resident provides their name, date of birth, gender, address and other optional fields such as mobile number, e-mail etc along with biometrics, namely, Photograph, 10 Finger prints and Iris. UIDAI will be responsible for safe custody of the information collected for the purpose of Aadhaar generation once it reaches CIDR.
- b) **Enrolment for the Registrars services** – In addition to the information being collected by UIDAI, the Registrars may also be collecting a wide range of information together with biometrics and the Aadhaar number in order to deliver their services to the residents. This information could be viewed as personal information. Hence, ensuring the confidentiality and security of this data is of great importance.

2. UIDAI responsibility for - data protection and security

UIDAI is capturing biometrics and demographics information to issue Aadhaar numbers to the residents and to authenticate the identity of an Aadhaar number holder. It is the responsibility of UIDAI to ensure safety and security of the data collected for Aadhaar enrolment. The data captured (demographic and biometric) shall at the point of collection be encrypted and transported to the Central Identities Data Repository where the UIDAI will decrypt the data in a secure location and use it for the purpose of de-duplication and subsequently for authentication. UIDAI will have a security policy in place which will detail and define the security protocols and access protocols to ensure safety of the data. It is the responsibility of the UIDAI to ensure the safety, security and confidentiality of the data from the point of receipt and in the CIDR and to protect the data from unauthorised access and misuse.

3. Registrars responsibility for – data protection and security

The Aadhaar enrolments will be done through the Registrars. The Registrars will also be collecting additional data from the resident in order to deliver their services to the resident. This relationship between the resident and the Registrar is independent of the UIDAI. As a consequence Registrars have a fiduciary responsibility and has to exercise a duty of care to secure and protect all the data (demographic and biometric) collected from the resident. UIDAI prescribes the following broad measures for data protection and security to be adopted by Registrars:

a) Care in collection:

- Registrars shall take all necessary precautions, in respect of information received or collected by it so as to ensure such information is properly and accurately recorded, collated and processed;

b) Process for access and updating:

- Registrars shall also establish and adopt procedures to disclose to a person, upon their request, their own information – subject to satisfactory identification (in order to ensure that information is not revealed to third parties)

c) Principles and procedures relating to data collection, use and processing

- Registrars must collect information from residents only for the purpose related to their functions.
- The individual from whom data is being collected should be informed of the purpose for which information is being collected and how the data will be used.
- Registrars should obtain appropriate and clear legal consent from the resident.
- Registrars must ensure that data collected and maintained by them is protected against any loss, or unauthorized access, or use, or modification or disclosure.
- Data provided by the resident to a Registrar should be used by the Registrar for the purpose envisaged. Resident must be made aware of any data sharing policies of the Registrar. While some form of sharing maybe part of the governance framework of governments – residents must be made aware of the same. Any other sharing beyond the governance framework must only be done with the explicit consent of the resident and for the explicit reason for which the consent is given.

d) Data security protocols

- Security protocols should be in place from the point of collection, transmission of data and to the final destination/ facility where the data will be stored.
- Data must be housed in a secure facility with appropriate access controls and audit trails.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful collection and processing of data and against accidental loss or destruction of, or damage to data.

e) Data retention policy

- Registrars must define the time period for which data is being collected and will be retained by them. Data should not be retained for longer than the purpose for which it was meant to be used.
- Data must not be made available for the use of or be retained by third party service providers such as enrolling agencies or by any other unauthorised personnel.
- Registrars must develop their own guidelines for preservation and destruction of data and records according to their functional needs.

4. Security framework for Biometric data

While the above broad guidelines are applicable for all forms of data collected from the residents, special care needs to be taken to address the security of biometric information. Biometrics is unique to an individual and therefore is sensitive information that needs to be protected with the highest standard of care to thwart any possibility of misuse.

The biometric data will be encrypted immediately upon capture during the enrolment process. The data packet will be encrypted with the Registrars key. The Registrar is responsible for the secure transmission of the data and for storing the data at a secure location protected from unauthorised access and misuse. The Registrar is liable to the resident and the public at large for safety, security and proper use of the Biometric data collected by it. The following guidelines are prescribed for the Registrars for security protocols relating to biometric information of the residents.

4.1 Guidelines

1. Registrars should inform residents what biometric data is being collected and how the data will be used.
2. Develop data use and retention policies - Registrars should not collect and retain more data than they need for their purpose (if they want to issue cards

and store finger print they should retain that data only and not the rest). Information that is not required must not be retained by them.

3. Registrars should develop data security policies and build up systems to ensure safe keeping of biometric data, protect from malware, spyware and hacking of systems, including access protocols, etc. For this purpose :
 - Registrars must have a physically secure location (data centre) where the biometric data can be housed, with strict security protocols and protection from unauthorised access. Physical, network and application security must be taken care of.
 - Biometric Data should always be stored in encrypted form. Data should not lie unencrypted at rest.
 - Biometric Data should not be decrypted except for the time when it is being used.
 - Only data that is required should be retained and the rest should be destroyed.
 - Key management systems with logging and audit trails should be created preferably using a Hardware Security Module (HSM).
 - Independent audit of the security facilities, processes and policies should be done periodically and reports should be published to assure the public of the safety standards being followed.

4. Biometric data should not be made available to or be retained by enrolling agencies, at user points or by any other unauthorised personnel.

5. Key technical safeguards

Overall objective

To ensure that all UIDAI Registrars meet a minimum level of security when they store, process and transmit resident data the UIDAI has prescribed following control objectives and recommendations to meet them :

Control Objectives	UIDAI Recommendations
Maintain an Information Security Policy	Maintain a policy that addresses information security
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software on all systems commonly affected by malware
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to resident data by business need-to-know
	Assign a unique ID to each person with

	computer access
	Restrict physical access to resident data
Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect resident data
	Do not use vendor-supplied defaults for system passwords and other security parameters
Regularly Monitor and Test Networks	Track and monitor all access to network resources and resident data
	Regularly test security systems and processes
Protect Resident Data	Protect stored resident data
	Encrypt transmission of resident data across open, public networks

Maintain an Information Security Policy

Registrars must create and maintain an information security policy, which addresses the security requirements arising out as a result of their functional/ business needs and objectives. The objectives of this security policy are to:

- Provide management direction and support for information security.
- Provide a baseline for information security. Partner will have the flexibility to modify components of the operational framework to take into account specific business objectives and security requirements.
- Ensure appropriate safeguards and procedures are adopted to protect information and associated information technology resources
- Ensure that persons handling information are aware of their accountability and responsibilities

This policy shall be implemented through a process approach, based on the PDCA (Plan, Do, Check, Act) as follows. Sample Policies and Procedures followed by other organizations are listed in the annexure .

- **Plan**
Establish a security policy, objectives, targets, processes and procedures relevant to managing risk, and information security to deliver results in accordance with the Partner's overall policies and objectives
- **Do**
Implement and operate the security policy, control processes and procedures.
- **Check**
Monitor, and review the Security policy, control processes and procedures

- **Act**

Take corrective and preventive actions based on audit and review to achieve continuous improvements of the security plan.

Maintain a Vulnerability Management Program

Registrars must formulate risk assessment policies, and procedures. As a part of this, all assets must be listed, threats & vulnerabilities identified, and assessed, and mitigation plan implemented for all threats. As a result of this, all vulnerable and high risk components would be identified, and protected. Some specific recommendations that may come out of such an exercise include:

- Use and regularly update anti-virus software on all systems commonly affected by malware. This includes all anti-spyware, anti-virus, and other host protection systems.
- Develop and maintain secure systems and applications. This includes the adoption of a secure software development life cycle.

Implement Strong Access Control Measures

Registrars must identify all information assets, and how they are used in their system. This must be followed by the following actions:

- Restrict access to resident data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to resident data

Access control must include physical, host (computer), and network security.

Build and Maintain a Secure Network

It is essential that a secure network be established to protect the system from attack, and misuse. Some sample guidelines for securing this network include:

- Install and maintain a firewall configuration to protect resident data. A firewall is required to prevent external, potentially malicious intruders from accessing the network, and the resources within.
- Do not use vendor-supplied defaults for system passwords and other security parameters. A commonly ignored aspect of security is that various systems come with default security parameters including passwords. Having them set to default values would allow intruders to access the network, and steal data / inflict damage.

Regularly Monitor and Test Networks

Once a secure network is established, it must be regularly monitored, and steps must be taken to keep it up-to-date for all security issues. Some possible mechanisms to ensure this include:

- Track and monitor all access to network resources and resident data
- Regularly test security systems and processes
- Regular security audits, and penetration tests for all systems, networks, and processes will help to keep security up to date with current threats, and ensure that no complacency sets in.

Protect Resident Data

From the resident's perspective, the primary purpose of all security plans is to ensure that the resident's data is not stolen, vandalized, or compromised in any way. To accomplish this, in addition to all the previous steps, the Registrar must classify resident data based on value, and usage. Further, a cryptographic system must be put in place

- Encrypt resident data at rest: i.e. all resident data must be encrypted, while it is stored on external or internal secondary storage.
- Encrypt resident data in motion: i.e. all resident data must be encrypted while it is being transmitted across open public networks (or even closed networks).
- Protect unencrypted data: i.e. while the data is in the host memory, unencrypted, the host system must be protected from malicious activity, including viruses, spyware, etc.

6. Compliance

Compliance can be summarized into 3 stages:

Collecting and storing: Secure collection and tamper-proof storage of all log data so that it is available for analysis.

Reporting: Being able to prove compliance on the spot if audited and present evidence that controls are in place for protecting data.

Monitoring and alerting: Have systems in place such as auto-alerting, to help administrators constantly monitor access and usage of data. Administrators are warned of problems immediately and can rapidly address them. These systems should also extend to the log data itself – there must be proof that log data is being collected and stored.

Compliance can be accessed through the use of an annual onsite data security audits, and quarterly network scans.

Annexure : List of Sample Policies which the Registrars must have in place:

- Information Security & Management Policy
- Information Security Organization Structure Policy
- Risk Assessment Policy & Procedures
- Asset Classification Policy and Procedure
- Asset Classification and control standard
- Information labeling and handling procedure
- Acceptable Use Guideline
- Procedure for control of documents and records
- Human Resources Security Policy and Procedure
- Physical and Environmental Security Policy and Procedure
- Change Management Policy and Procedure
- Third Party Management Policy and Procedure
- Antivirus and Malicious Software Policy and Procedure
- Backup and Restore Policy and Procedure
- Network Security Policy and Procedure (Including internet, intranet, mobile computing, tele-working, firewall security)
- Media Handling Policy and Procedure
- Monitoring Policy and Procedure
- Access Control Policy and Procedure (including password security)
- Network Access Control Policy and Procedure
- Systems Development Maintenance Policy and Procedure
- Incident Management Policy and Procedure
- Business Continuity Management Policy and Procedure
- Cryptographic procedure document
- Minimum Baseline Security Standards