Version 1.0

Department of Information Technology & Communication
Government of Rajasthan

INFORMATION SECURITY POLICY- AADHAAR AUTHENTICATION ECOSYSTEM
ASA/KSA (AUTHENTICATION SERVICE AGENCY/KYC SERVICE AGENCY)

Contents

Document Version Details		
Version	**Creator**	**Reviewer/Approver**
1.0	Pankaj Jaldeep, ACP(DD) Date: 15-04-2025	**Reviewed by-** Sh. Anil Singh, Director (Technical), RISL & CISO, Rajasthan. **Date:** 08-05-2025 **Approved by-** Secretary & Commissioner, IT&C **Date:** 09-05-2025

Statement of Confidentiality

This document presents the Information Security Policy of UIDAI for external ecosystem partners ASA and contains information that is proprietary and confidential to UIDAI. Any use or disclosure in whole or part of this information for any reason without written permission of UIDAI is strictly prohibited.

Foreword

The UIDAI ecosystem is one of the most complex environments in the world today. The entire backbone of this ecosystem is the residents' identity Information, which is created, processed, transmitted, stored and securely disposed by UIDAI and Its ecosystem partners. Hence, it is imperative to define and implement robust controls to safeguard the residents' identity information, and create trust between the residents and the UIDAI ecosystem against the misuse of such information.

UIDAI has defined a set of people, process and technical controls to govern the use of this information, in alignment with industry standards such as ISO 27001. Focus of this document is to protect residents' information and the information infrastructure, build capabilities to prevent and respond to information security threats, eliminate identified vulnerabilities and minimize damage from information security incidents through a combination of institutional structures, people, processes and technology.

This Information Security policy document specifies the scope and the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the Information Security environment/landscape of Unique Identification Authority of India (UIDAI).

1. Policy Statement

Department of Information Technology & Communication (DoIT&C), Govt. of Rajasthan is registered as an AUA/KUA (Authentication User Agency/KYC User Agency) and ASA/KSA (Authentication Service Agency/KYC Service Agency) with Unique Identification Authority of India (UIDAI), GoI. Security of UIDAI information assets handled by the external ecosystem partners i.e. AUA/KUA for providing services is of paramount importance. The confidentiality, integrity and availability of these shall always be maintained by AUA/KUA by deploying controls commensurate with the asset value.

1.1 Control Objective

DoIT&C shall ensure the security of UIDAI information assets handled by DoIT&C- ASA/KSA:

1. Providing DoIT&C- ASA/KSA with an approach and directives for implementing information security of all information assets used by them for providing services to UIDAI and AUAs/KUAs;

2. Establishing review mechanism to ensure that the DoIT&C- ASA/KSA adhere to all provisions of the UIDAI Information Security Policy – External Ecosystem ASA/KSA.

1.2 Scope

This policy is applicable to all DoIT&C-Authentication Service Agency/KYC Service Agency that provide CIDR connectivity to AUAs/KUAs.

1. **Authentication Service Agency (ASA) & KYC Service Agency (KSA):** ASAs/KSAs are agencies that have established secured leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to requesting entities (such as AUAs/KUAs) and transmit their authentication requests to CIDR.

DoIT&C- AUA/KUA connects to the Central Identities Data Repository (CIDR) through DoIT&C- ASA/KSA. ASAs have established secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications. ASAs offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (AUA) and transmit AUAs' authentication requests to CIDR. Only agencies contracted with UIDAI as ASAs shall send authentication requests to the CIDR; no other entity can directly communicate with CIDR. An ASA could serve several AUAs; and may also offer value added services such as multi-party authentication, authorization and MIS reports to AUAs.

This Policy is applicable wherever UIDAI information is processed and/or stored by DoIT&C- Authentication Service Agencies. Authentication Service Agencies shall ensure the confidentiality, integrity, and availability of UIDAI related data and services.
In case there is a conflict of any of the provisions of this policy with the Aadhaar Act, 2016 or its Regulations, then the Aadhaar Act, 2016 and Regulations shall prevail.

2. Information Security policy for DoIT&C- ASA/KSA

2.1 Purpose

This section outlines the Information Security policy and Information Security controls applicable to DoIT&C- ASA/KSA.

2.2 Terms and Definitions

S. No.	Terms	Definitions
1	AAS	AADHAAR Authentication Server
2	ADG	Assistant Director General
3	AUA/ASA	Authentication User Agency/Authentication Service Agency
4	CA	Certifying Authority
5	CCTV	Closed Circuit Television
6	CIDR	Central Identities Data Repository
7	CN	Common Name
8	DDG	Deputy Director General
9	eKYC	Electronic Know Your User
10	GRC	Governance, Risk and Compliance
11	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.)
12	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 architecture, infrastructure, network details etc.
13	IDS	Intrusion Detection System
14	ISO (ISO27001)	International Organisation of Standardization
15	IT	Information Technology
16	IPS	Intrusion Prevention system
17	KUA	Know your customer User Agencies
18	NDA	Non-Disclosure Agreement

19	NTP	Network Time Protocol
20	PID	Personal Identity Data
21	PII	Personally Identifiable Information
22	SPOC	Single Point of Contact
23	SSL	Secure Sockets Layer
24	STQC	Standard testing and quality control
25	TSU	Technical Support Unit
26	VA	Vulnerability Assessment
27	VPN	Virtual Private Network
28	WAF	Web Application Firewall

2.3 Human Resources

1. DoIT&C-ASA shall appoint a SPOC/team for all UIDAI related activities and communication with UIDAI. Office In-charge, Aadhaar Authentication project shall act as SPOC.
2. DoIT&C-ASA shall conduct a background check or sign an agreement/NDA with all personnel/agency handling Aadhaar related authentication data. UIDAI or agency appointed by UIDAI may validate this information.
3. An induction as well as periodic functional and information security trainings shall be conducted for all DoIT&C-ASA personnel for UIDAI related services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
4. All employees accessing UIDAI information assets shall be made aware of UIDAI information security policy and controls.

2.4 Asset Management

1. All assets used by the DoIT&C-ASA (servers, network devices, etc.) for the purpose of delivering services to UIDAI shall be identified, labelled and classified. Details of the information asset shall be recorded.
2. The assets which are scheduled to be disposed must have a procedure as part of the disposal policy of the DoIT&C. Information systems containing UIDAI information shall be disposed-off securely only after obtaining approvals from UIDAI authorized personnel.
3. Before sending any equipment out for repair, the equipment shall be sanitised to ensure that it does not contain any UIDAI sensitive data.
4. DoIT&C-ASA shall implement controls to prevent and detect any loss, damage, theft or

compromise of the assets.

2.5 Access Control

1. Only authorized individuals shall be provided access to information assets (such as servers, network devices etc.) processing UIDAI information.
2. DoIT&C-ASA personnel with access to UIDAI information assets shall:
    a) Have least privilege access for information access and processing;
    b) The operator must be logged out after the session is finished.
3. The systems should have auto lock out feature i.e. after a certain time of inactivity (15 mins or as specified in the DoIT&C-ASA policy document), the system should log out;
4. Access rights and privileges to information assets for UIDAI information shall be revoked within 24 hours' separation of respective personnel or as mentioned in the exit management policy of the organization. Post deactivation, user IDs shall be deleted if not in use as per Exit formalities;
5. Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for audit purposes;
6. Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approved and documented where there is no alternative;
7. Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems.
8. The users should not be provided with local admin access rights on their system. In the case of administrative access being provided, the users shall be prohibited from modifying the local security settings. Modifying the same shall result in disciplinary action.
9. Three successive login failures or as per the access control policy/password policy of the organization should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications there should be an automatic lock out period of 30 mins in case of three consecutive login failures or as per the access control policy/password policy of the organization.
10. The local security settings on all the systems shall be aligned and synced with the Active Directory or similar solutions for group policy enforcement.

2.6 Password Policy

1. Password policy defined in Rajasthan E-governance IT & ITes Policy-2015 shall be applicable. https://doitc.rajasthan.gov.in/writereaddata/PoliciesGuidelinesOrders/20210908121041649134 0ITPolicy2015.pdf

2.7 Cryptography and Security of Aadhaar number

2. While establishing a secure channel to the AADHAAR Authentication Server (AAS), the DoIT&C-ASA shall verify the following:
    a) The digital certificate presented by the AAS has been issued /

signed by a trusted Certifying Authority (CA);

b) The digital certificate presented by the AAS has neither been revoked nor expired;

c) The Common Name (CN) on the certificate presented by the AAS matches with its fully qualified domain name (presently, auth.uidai.gov.in);

3. Key management activities shall be performed by DoIT&C-ASA to protect the keys throughout their lifecycle. The activities shall address the following aspects of key management, including;
    a) key generation;
    b) key distribution;
    c) Secure key storage;
    d) key custodians and requirements for dual Control;
    e) prevention of unauthorized substitution of keys;
    f) Replacement of known or suspected compromised keys;
    g) Key revocation and logging and auditing of key management related activities.
4. Encrypted PID block and license keys that came as part of authentication packet should never be stored anywhere in its system.

2.8 Physical and Environmental Security

1. The DoIT&C-ASA servers/network equipment should be placed in a secure lockable cage in the ASA data center.
2. The facility should be manned by security guards during and after office hours.
3. CCTV surveillance shall cover the ASA servers.
4. Access to the premises should be limited to authorised personnel only and appropriate logs for entry of personnel should be maintained.
5. The movement of all incoming and outgoing items shall be documented;
6. Lockable cabinets or safes shall be provided in the offices, rooms and information processing facilities for critical information storage especially for UIDAI related documents as applicable.
7. Fire doors and extinguishing systems shall be deployed, labeled, monitored, and tested regularly;
8. Preventive maintenance activities like audit of fire extinguishers, CCTV should be periodically done.
9. Physical access to restricted areas or offices and facilities hosting critical equipment shall be pre-approved and recorded along with the date, time and purpose of entry
10. Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall be posted at all entrances and at other points along the restricted areas as necessary especially where the ASA servers/network equipment are physically hosted.
11. Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage;

12. A clear desk and clear screen policy for UIDAI information processing facilities shall be adopted to reduce risks of unauthorized access, loss and damage to information related to UIDAI. Following shall be ensured:
    a) Screen saver or related technological controls shall be implemented to lock the screen of the information systems when unattended beyond a specified duration;
    b) Unused paper documents and printed papers shall be shredded.

2.9 Operations Security

1. DoIT&C-ASA shall only engage with the AUAs / KUAs approved by UIDAI and keep UIDAI informed of the list of AUAs it serves. In case of disengagement with an AUA / KUA, the ASA shall inform UIDAI within a period of 7 days from the date of disengagement;
2. Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure;
3. Where segregation of duties is not possible or practical, the process shall include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision;
4. The Test and Production facilities / environments must be physically and/or logically separated.
5. DoIT&C-ASA personnel shall conduct integrity checks to verify the completeness of the data packet and authenticity of the authentication user agency before processing the authentication request. A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level;
6. Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
7. DoIT&C-ASA employees shall not intentionally write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID information;
8. DoIT&C-ASA servers connected to the CIDR shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed;
9. Network intrusion and prevention systems should be in place – e.g. IPS, IDS, WAF, etc.
10. DoIT&C-ASA shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring;
11. Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only;
12. The authentication audit logs should contain, but not limited to, the following transactional

details:

- Identity of the requesting entity
- Parameters of authentication request submitted
- Parameters received as authentication response

13. Aadhaar number, PID information, device identity related data and eKYC response data shall not be retained in the DoIT&C-ASA logs.
14. The logs of authentication transactions shall be maintained by the DoIT&C-ASA for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
15. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations governing the DoIT&C-ASA, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes.
16. All server/network devices clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation;
17. The DoIT&C-ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organisation i.e. DoIT&C; The DoIT&C-ASA server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities;
18. Service Continuity and service availability shall be ensured through DR site.

2.10 Communications Security

1. The network between AUA / KUA and DoIT&C-ASA shall be secured. AUA / KUA shall connect with DoIT&C-ASA through leased lines or similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.
2. The network between DoIT&C-ASA and CIDR shall be secure. DoIT&C-ASA shall connect with CIDR through leased lines or similar secure private lines.
3. The DoIT&C-ASA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the server from all sources other than the respective AUAs / KUAs
4. The DoIT&C-ASA server host shall reside in a segregated network segment that is isolated from the rest of the network of the ASA organisation i.e. DoIT&C;
5. Non-essential services shall be disabled on all information systems;
6. Use of e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy Information Security Incident Management.
7. DoIT&C-ASA shall be responsible for reporting any security weaknesses, any incidents, possible misuse or violation of any of the stipulated guidelines to UIDAI immediately.

2.11 Compliance

1. DoIT&C-ASA shall comply with all terms and conditions outlined in the UIDAI ASA agreement and ASA compliance checklist.
2. DoIT&C-ASA shall ensure that its operations are audited by an information system auditor certified by a recognized body on an annual basis and on need basis to ensure compliance with standards and specifications. The audit report shall be shared with UIDAI upon request;
3. If any non-compliance is found as a result of the audit, management shall:
    a) Determine the causes of the non-compliance;
    b) Evaluate the need for actions to avoid recurrence of the same;
    c) Determine and enforce implementation of corrective action;
    d) Review the corrective action taken.
4. UIDAI shall reserve right to audit systems and processes of the DoIT&C-ASA on an annual basis and as needed to ensure compliance with stipulated security guidelines. The audit plan shall include information security controls audit and technical testing including vulnerability assessment as well as penetration test of Information Systems and any new technology or delivery channel introduced;
5. DoIT&C-ASA shall use only licensed software within the UIDAI network environment. Record of all software licenses shall be kept and updated regularly;
6. DoIT&C-ASA and their partners shall ensure compliance to all the relevant laws, rules and regulations, including, but not limited to, ISO27001: 2013 Standard, IT Act 2000 and 2008 amendments; It is recommended that ASA shall deploy as part of its systems, a Fraud Analytics module that is capable of analyzing authentication related transactions to identify fraud.
7. DoIT&C-ASA must have their authentication servers routing to CIDR hosted in data centers within India.
8. Ensure that all infrastructure and operations including systems, processes, devices, software and biometric infrastructure, security, and other related aspects, are in compliance with the standards and specifications as may specified by the Authority for this purpose;
9. DoIT&C-ASA shall at all times, comply with directions, specifications, etc. issued by the Authority, in terms of network and other Information Technology infrastructure, processes, procedures, etc.
10. DoIT&C-ASA shall comply with all relevant laws and regulations relating, in particular, to data security and data management.
11. ASA shall be responsible to the Authority for all its authentication related operations, even in the event the ASA sub-contracts parts of its operations to other entities, the responsibility shall remain with the ASA.

2.12 Change Management

1. ASAs shall document all changes to UIDAI Information Processing facilities/ Infrastructure/

processes;

2. Change log/ register shall be maintained for all changes performed.

==========END OF DOCUMENT==========