Unique Identification Authority of India (UIDAI)

UIDAI Information Security Policy – External Ecosystem – Authentication User Agency/ KYC User Agency v6.0

Document Control

Sr No	Type of Information	Document Data
1	Document Title	UIDAI Information Security Policy – External Ecosystem – AUA/KUA
2	Document Code	UIDAI IS Policy/ External/AUA KUA/05
3	Date of Release	21st February 2023
4	Document Superseded	UIDAI Information Security Policy v5.0
5	Document Revision no	6.0
6	Document Owner	Director, Authentication & Verification, UIDAI
7	Document Author(s)	IS Division, UIDAI
8	Document Approvers	CEO, UIDAI

Document Change Approvals

Version No	Revision Date	Nature of Change	Date approved
Version 1.1	01-Dec-2011	First version (2011)	December-2011
Version 2.0	08-May-2014	• Alignment with ISO 27001:2013 requirements • Segregation of Control Statements from the Procedures and Guidelines • Addition of Information Security Governance Framework • Updating of security policies for UIDAI external ecosystem	27-Oct-14
Version 3.0	23-Jan-2015	Revision of Governance framework (ISMS) for stage I ISO27001:2013	02-Feb-15
Version 3.1	27-Feb-2015	Update of Annexure documents as per stage-2 comments	24-Apr-15
Version 3.2	22-Dec-2015	Creation of separate booklet from existing UIDAI information security policy document for external ecosystem partner for Authentication – AUA and KUA	No. F-11014/06/2014-Tech (Vol-II)/631 Dated 27th April 2016
Version 3.3	28-Feb-2017	Annual review	F. No. T-11011/23/2010-Tech Dated – 17 Jan 2019
Version 3.4	28-Feb-2018	Annual review • Included security provisions as per latest circulars, guidelines and notices issued	F. No. T-11011/23/2010-Tech Dated – 17 Jan 2019

		by UIDAI	
Version 3.5	02-Jan-2019	Annual Review • Included security provisions as per latest circulars, guidelines and notices issued by UIDAI	F. No. T-11011/23/2010-Tech Dated – 17 Jan 2019
Version 4.0	07-Feb-2020	• Change of CEO name from Shri. A. B. Pandey to Pankaj Kumar • Removed controls which are not required/applicable to the current environment • Application security controls added in section 2.10 • Data protection clauses added in Section 2.14	July 30, 2020
Version 5.0	03-April-2022	• Document Author name has been changed from "IS Division (Ashish Kandari, Navin Gupta)" to "IS Division (Rajeev Kumar)" • Document Approver name has been changed from "Shri Pankaj Kumar (CEO)" to "Shri Saurabh Garg (CEO)" • Changed control in Section 2.8 (Sr. no. 4) - Physical and Environmental Security and Section 2.9(Sr. no. 9) - Operations Security	06-April-2022
Version 6.0	15-February-2023	• Document Owner name has been changed from "Smt. Deepali Sharma, ADG (Authentication), UIDAI" to "Director Authentication & Verification, UIDAI" • Document Author name has been changed from "IS Division (Pradeep Singh)"to "IS Division, UIDAI". • Document Approver format has been changed from "Shri Saurabh Garg" to	Dated – 6 March 2023

		"CEO, UIDAI". • Inclusion of "Aadhaar (Authentication & Offline Verification) Regulations, 2021" wherever applicable. • Addition in Sec. 2.6 Password Policy (Point 4, 6 & 10). • Addition in Sec. 2.8 Physical and Environment Security (Point 4).	

Statement of Confidentiality

This document presents the Information Security policy of UIDAI for external ecosystem partner AUA/KUA 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.

February 2023, UIDAI

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/IEC 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 (hereafter referred as 'UIDAI').

Contents

1. Policy Statement

Security of UIDAI information assets handled by the external ecosystem partners for providing services, is of paramount importance. The confidentiality, integrity and availability of these shall always be maintained by these partners by deploying controls commensurate with the asset value.

1.1 Control Objective

UIDAI shall ensure the security of UIDAI information assets handled by AUA/KUA:

1. Providing AUA/KUA with an approach and directives for deploying security controls for all information assets used by them for providing services.
2. Establishing review mechanism to ensure that the AUA/KUA adhere to all provisions of the UIDAI Information Security policy for AUA/KUA as well as maintain compliance with the Aadhaar Act 2016 and its regulations.

1.2 Scope

The UIDAI Information Security policy – External Ecosystem Partner AUA/KUA is applicable to all AUA/KUA that provide services to UIDAI.

1. **Authentication User Agencies (AUA):** Authentication User Agency is a requesting entity that uses the Yes/ No authentication facility provided by UIDAI; and
2. **KYC User Agencies (KUA):** KYC User Agency is requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by UIDAI.

AUA connects to the Central Identities Data Repository (CIDR) through ASA (either by becoming ASA on its own or contracting services of an existing ASA). AUA/KUA uses demographic data, and/or biometric data in addition to the resident's UID. They use Aadhaar authentication to provide services such as opening of bank account, LPG connection, etc. to Indian residents. Since the AUAs handle sensitive personal data (e.g., biometrics), Aadhaar number, eKYC data etc. of the residents, it becomes imperative to ensure its security.

This policy is applicable wherever Aadhaar related information is processed and/or stored by AUA/KUA. 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 Authentication User Agencies (AUAs)/KYC User Agencies (KUAs)

2.1 Purpose

This section outlines the Information Security policy and Information Security controls applicable to Authentication User Agencies (AUAs) / KYC User Agencies (KUAs), Sub – AUAs and other sub-contractors of AUA /KUA handling Aadhaar authentication.

2.2 Terms and Definitions

S.No.	Terms	Definitions
1	API	Application Program Interface
2	AUA/ASA	Authentication User Agency/ Authentication Service Agency
3	BC	Business Correspondent
4	Biometric	Photograph, fingerprint, iris scan, or such other biological

	Information	attributes of an individual as may be specified by regulations
5	CA	Certifying Authority
6	CCTV	Closed Circuit Television
7	CIDR	Central Identities Data Repository
8	Demographics	Information relating to the name, date of birth, address and other relevant information of an individual as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history
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: a. Paper assets: (legal documentation, manuals, policies & procedures, organizational documents etc.) b. Physical assets: (computer equipment, communications, utility equipment, buildings etc.) c. Software assets: (database information, applications, software code, development tools, operational software etc.) d. People assets: UIDAI human resources and stakeholders e. Service assets: (logistics, building management systems, communications, utilities etc.)
12	HSM	Hardware Security Module
13	information/ information asset	Information that has value to the organization (UIDAI) including but not limited to resident biometric and demographic information, personally identifiable information, employee information, organization information such as CIDR architecture, infrastructure, network details etc.
14	IDS	Intrusion Detection System
15	IPS	Intrusion Prevention System
16	ISO	Information security division
17	ISO (ISO 27001)	International Organisation of Standardization
18	IT	Information Technology
19	KUA	Know your customer User Agencies
20	NDA	Non-Disclosure Agreement
21	NTP	Network Time Protocol
22	Personal data	Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.
23	PID	Personal Identity Data
24	PoT	Point of Transaction
25	Sensitive Personal Data	Personal data, which may, be related to, or constitute – a. Financial data; b. Health data; c. Official identifier; d. Sex life;

		e. Sexual orientation; f. Biometric data; g. Genetic data; h. Transgender status; i. Intersex status; j. Caste or tribe; or k. Religious or political belief or affiliation.
26	SOP	Standard Operating Procedures
27	SPOC	Single Point of Contact
28	SSL	Secure Sockets Layer
29	STQC	Standard testing and quality control
30	VA	Vulnerability Assessment
31	VID	Virtual ID
32	VPN	Virtual Private Network
33	WAF	Web Application Firewall

Information Security Domains and related Controls

2.3 Human Resources

1. AUA/KUA shall appoint a Technical and Management SPOC for Aadhaar related activities and communication with UIDAI. AUA/KUA shall also inform UIDAI about the appointment of any new SPOC.
2. AUA/KUA shall conduct a background check and sign a confidentiality agreement/NDA with all personnel/agency handling Aadhaar related information. UIDAI or agency appointed by UIDAI may validate this information.
3. AUA / KUA shall take an undertaking from BCs / similar entities (if applicable), Sub-AUAs and other third-party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data.
4. Information security and data privacy trainings shall be conducted by the AUA for all sub AUAs personnel for Aadhaar related authentication services during induction and subsequently on periodic basis. The training shall include all relevant security and data privacy guidelines as per the UIDAI information security policy for Authentication, Aadhaar Act, 2016, Aadhaar (Authentication & Offline Verification) Regulations, 2021 and all circulars/notices published from time to time.
5. Specific and specialised training shall be conducted for various functional roles involved in authentication ecosystem.
6. Training shall be conducted half yearly and as and when changes are made in the authentication ecosystem. AUA/KUA shall maintain records of such trainings conducted.
7. Access to authentication infrastructure shall not be granted before signing NDA and completion of BGV for personnel.
8. The user ID credentials and access rights of personnel handling Aadhaar related authentication data shall be revoked/ deactivated within 24 hours of exit of the personnel.

2.4 Asset Management

1. All assets used by the AUA/ KUA (business applications, operating systems, databases, network etc.) for the purpose of delivering services to residents using Aadhaar authentication services shall be identified, labelled and classified.
2. Details of the information asset shall be recorded, and an asset inventory should be maintained and updated as and when required.
3. AUA/KUA shall define a procedure for disposal of the information assets being used for authentication operations. Information systems / documents containing Aadhaar related information shall be disposed-off securely.
4. Before sending any equipment out for repair, the equipment shall be sanitised to ensure that it does not contain any Aadhaar related data. A movement log register of all the equipment sent outside shall be maintained.
5. AUA / KUA shall not transfer or make an unauthorized copy of any Aadhaar related information including identity information to any personal device or other unauthorized electronic media / storage devices.
6. AUA / KUA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets containing any Aadhaar related information.
7. AUA / KUA shall ensure that authentication devices used to capture resident's biometric are STQC certified registered devices. AUA/KUA shall also ensure that all the Sub-AUAs, Business Correspondents or other sub-contractors also use the STQC certified registered devices only.
8. Ownership of authentication assets shall be clearly defined and documented.
9. All the assets (e.g., PoS devices, tablets, desktop, laptop, servers, databases etc.) used by AUA/KUA and their sub-contractors for Aadhaar authentication shall be used after their hardening has been done as per the AUA/KUA hardening baseline document. AUA / KUA shall define their own hardening standards, unless specified by UIDAI.

2.5 Access Control

1. Only authorized individuals shall be provided access to information facilities (such as authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information. Access control list shall be maintained by AUA/KUA.
2. AUA / KUA, sub-AUA, BC and other third-party personnel with access to UIDAI information assets shall have least privilege access for information access and processing.
3. Access rights and privileges to information processing facilities for Aadhaar related information shall be revoked within 24 hours of exit of respective personnel. Post deactivation, user IDs shall be deleted if not in use.
4. Access rights and privileges to information facilities processing Aadhaar related information shall be reviewed on a quarterly basis and the report shall be maintained for audit purposes.
5. Common user IDs / group user IDs shall not be used. Exceptions shall be approved by AUA/KUA's senior management and documented where there is no alternative.
6. Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems; if done manually, then a fireproof safe or a password vault shall be used, and an access log register shall be maintained.

7. The users shall 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.
8. In the case of assisted devices and applications where operators need to mandatorily perform application functions (not a self-service application), operators should be authenticated using some authentication scheme such as password, Aadhaar authentication, smart card-based authentication, etc.
9. Three successive login failures shall result in user account being locked; they should not be able to login until their account is unlocked and the password reset. The user shall have to contact the System Engineers/Administrators for getting the account unlocked.

2.6 Password Policy

1. The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login.
2. All user passwords (including administrator passwords) shall remain confidential and shall not be, written, shared, posted or otherwise divulged in any manner.
3. If the passwords are being stored in the database or any other form, they should be stored in an encrypted / hashed form.
4. Two/Multi-factor authentications shall be enabled in critical infrastructural components and to areas where confidential information is processed or stored.
5. Password shall be changed whenever there is any indication of possible system or password compromise.
6. Complex passwords shall be selected with a minimum length of 14 characters, which:
   a. are not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
   b. is free of consecutive identical characters or all-numeric or all-alphabetical groups;
   c. contains at least one numeric, one uppercase letter, one lowercase letter and one special character;
   d. shall be changed at regular intervals (passwords for privileged accounts shall be changed more frequently than normal passwords);
   e. shall not allow the use of last 3 passwords;
   f. shall not allow the username and password to be the same for a particular user; and
   g. users shall not use the same password for various UIDAI access needs.
7. Passwords shall not be hardcoded in codes, login scripts, any executable program or files.
8. Password should not be stored or transmitted in applications in clear text or in any reversible form.
9. Password shall not be included in any automated log-on process, e.g. stored in a macro or function key.
10. The application should have auto lockout feature i.e., after a certain time of inactivity (15 mins or as specified in the policy document), the session should logout.

2.7 Cryptography and Security of Aadhaar number

1. The Personal identity data (PID) block comprising of the resident's demographic / biometric data shall be encrypted as per the latest API specifications rolled out by UIDAI.

2. The PID shall get encrypted at the end point device used for authentication and it shall remain encrypted during transit and flow within the AUA / KUA ecosystem and while sharing this information with ASAs.
3. The encrypted PID block shall not be stored unless in case of buffered authentication for not more than 24 hours after which it should be deleted from the local systems.
4. AUA/KUA while providing authentication services to Sub-AUAs / other subcontracted entities shall ensure that the client application used for Aadhaar authentication is developed by AUA/KUA and is digitally signed by the AUA/KUA.
5. The key(s) used for digitally signing of authentication request and decryption of e-KYC XML Response shall be stored in HSM only. The HSM used shall be FIPS 140-2 compliant.
6. The AUA/KUA shall follow all the HSM provisions as defined in the circular – 11020/204/2017 dated 22nd June 2017 and any subsequent guideline / circular / notice published by UIDAI in this regard.
7. The authentication request shall be digitally signed by the requesting entity and/or by the Authentication Service Agency, as per the mutual agreement between them.
8. Key management activities shall be performed by all AUA / KUA 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 compromised or suspected compromised keys; and
   g. Key revocation and logging and auditing of key management related activities.
9. The Reference Key used for Aadhaar Data Vault should be generated using Universally Unique Identifier (UUID) scheme so that Aadhaar Number can neither be guessed nor reverse engineered using the reference.
10. Full Aadhaar number display must be controlled only for the Aadhaar number holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked such that only last four digits of the Aadhaar number are displayed.
11. Global and local AUA shall make necessary changes in their authentication systems for use of Virtual token, UID token and Limited e-KYC.
12. AUA/KUA shall integrate Virtual Token and UID Token into their services.

2.8 Physical and Environmental Security

1. The AUA/KUA servers should be placed in a secure cabinet in the AUA Data Centre.
2. AUA/KUA Data Center hosting Aadhaar related information shall be fully secured, and access controlled.
3. AUA/KUA Data Center shall be manned by security guards during and after office hours.
4. AUA/KUA shall retain the recordings of CCTV for at least 90 (Ninety) days. Further, access to CCTV logs and recordings shall be provided to authorized individuals only. CCTV recordings shall be securely stored and in case of any breach or incident, these recordings shall be shared upon request with UIDAI. Backup of CCTV shall be retained in media for 1 (one) year.
5. Access to the AUA/KUA Data Center shall be limited to authorized personnel only and appropriate logs for entry of personnel should be maintained.

6. The movement of all incoming and outgoing assets related to Aadhaar in the AUA/KUA Data Center shall be documented.
7. Lockable cabinets or safes shall be provided in the AUA/KUA Data Center and information processing facilities having critical Aadhaar related information.
8. Fire doors and fire extinguishing systems shall be deployed, labelled, monitored, and tested regularly.
9. Preventive maintenance activities like audit of fire extinguishers, CCTV shall be conducted quarterly.
10. Physical access to AUA Data Center and other restricted areas hosting critical Aadhaar related equipment/information shall be pre-approved and recorded along with the date, time and purpose of entry.
11. 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 AUA/KUA servers are physically hosted.
12. Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage.
13. A clear desk and clear screen policy shall be adopted to reduce risks of unauthorized access, loss and damage to information related to Aadhaar. Screen saver or related technological controls shall be implemented to lock the screen of the information systems when unattended beyond a specified duration.
14. Controls such as intrusion detection and evaluation plans shall be implemented in case of an emergency.

2.9 Operations Security

1. AUA/KUA shall complete the Aadhaar AUA / KUA on-boarding process as defined by UIDAI, before the commencement of formal operations.
2. Information security policy, processes, roles and responsibilities for Information security shall be maintained by AUA/KUA for governance of Information security.
3. Standard Operating Procedure (SOP) shall be developed for all information systems and services related to Aadhaar 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.
4. Personnel involved in operational/development/testing functions shall not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or process and which may compromise data security requirements.
5. 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.
6. AUA / KUA personnel 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 Aadhaar information.
7. The Test and Production facilities / environments must be physically and/or logically separated.
8. 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.

9. Vulnerability assessment exercise should be conducted at least on an Annual basis for ensuring the security of the Aadhaar infrastructure. Reports shall be generated and shared upon request with UIDAI.
10. All hosts that connect to the Aadhaar Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. Anti-virus / malware detection software shall be installed on such hosts.
11. Network intrusion and prevention systems should be in place – e.g., IPS, IDS, WAF, etc.
12. AUA/KUA 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.
13. 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.
14. The AUA/KUA shall follow all the consent related provisions as defined in the Aadhaar Act, 2016, Aadhaar (Authentication & Offline Verification) Regulations, 2021 and all circulars/notifications published from time to time.
15. The AUA/KUA shall maintain the logs of the Aadhaar authentication transaction as defined in the Aadhaar (Authentication & Offline Verification) Regulations, 2021.
16. The Aadhaar authentication logs shall not, in any event, retain the PID information.
17. The e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, shall be stored in encrypted form after obtaining appropriate consent from the resident. Further, the usage of e-KYC data shall be governed as defined by the Aadhaar Act 2016, Aadhaar (Authentication & Offline Verification) Regulations, 2021 and all circulars/notifications published from time to time.
18. The e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, shall be shared with sub-AUA or any other entity after obtaining specific permission from UIDAI by submitting an application in this regard. After obtaining the appropriate permissions, the said data may be shared as per provisions of the Aadhaar Act, 2016, Aadhaar (Authentication & Offline Verification) Regulations, 2021 and all circulars/notifications published from time to time.
19. The client application used for Aadhaar authentication by AUA/KUA and its ecosystem partners should not store biometric data collected during authentication under any circumstances.
20. The logs of authentication transactions shall be maintained by the AUA/KUA as defined by Aadhaar Act,2016, Aadhaar (Authentication & Offline Verification) Regulations, 2021 and all circulars/notifications published from time to time.
21. The AUA / KUA server shall reside in a segregated network segment that is isolated from the rest of the network of the AUA / KUA organisation. The AUA / KUA server shall be dedicated for the online Aadhaar authentication purposes and shall not be used for any other activities not related to Aadhaar.
22. All computer 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.
23. AUA/KUA, sub-AUAs, BCs and other sub-contractors performing Aadhaar authentication shall ensure identity information is not displayed or disclosed to external agencies or unauthorized persons. Also, Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate or any other document/service shall not be published or displayed at any platform.

24. No data pertaining to the resident or the transaction shall be stored within the terminal device.
25. Global AUAs and KUAs shall store Aadhaar numbers and Aadhaar related information on a separate secure database / vault / system, which shall be made secure and accessed through internal systems only. This Aadhaar Data Vault must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.
26. Aadhaar number and any other data kept in the Aadhaar Data Vault shall be kept in an encrypted format only.
27. The AUA/KUA shall follow all the Aadhaar Data Vault provisions as defined in the circular – 11020/205/2017 dated 25th July 2017 and any subsequent guideline / circular / notice published by UIDAI in this regard.
28. The AUA/KUA may be collecting biometric of residents for purposes other than those defined under the Aadhaar Act 2016, Aadhaar (Authentication & Offline) Verification Regulations, 2021 and all circulars/notifications published from time to time. In such cases, Aadhaar number should not be linked with the biometric data collected for such other purposes.
29. The user account shall be logged out after the session is finished.
30. An auto lock out mechanism for workstation, servers and/ or network device shall be implemented.
31. KUA shall not share its e-KYC license key with any other organisation. Sub-AUAs or any other entity shall not perform e-KYC using a KUA's license key.
32. For better decoupling and independent evolution of various systems, it is necessary that Aadhaar number be never used as a domain specific identifier. In addition, domain specific identifiers need to be revoked and/or re-issued.
33. Separate license keys must be requested by AUA for their Sub-AUAs, via UIDAI Auth-Support <authsupport@uidai.gov.in> .
34. AUA / KUA must have its Aadhaar related servers hosted in data centers within India.
35. AUA/KUA shall perform source code review of the modules and applications used for Authentication and e-KYC as well as vulnerability assessment, penetration testing and configuration assessment of the infrastructure.

2.10 Application Security

1. AUA/KUA shall ensure that all pages and resources of the modules and application used for authentication and e-KYC by default require authentication except those specifically intended to be public.
2. AUA/KUA shall further ensure that there are no default passwords in use for the application framework or any components used by the application.

2.11 Communications Security

1. Each authentication device shall have a Unique Device Code. This number shall be transmitted with each transaction along with UIDAI assigned institution code for the AUA / KUA as specified by the latest UIDAI API documents.
2. A unique transaction number shall be generated automatically by the authentication device which should be incremented for each transaction processed.
3. The network between AUA / KUA, its sub-contractors and ASA shall be secure. AUA / KUA shall connect with ASAs 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.

4. The AUA / KUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA / KUA server from all sources other than AUA/KUA's PoT terminals.
5. Use of web-based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy.

2.12 Information Security Incident Management

1. AUA / KUA shall be responsible for reporting any security weaknesses, incidents, possible misuse or violation of any of the stipulated guidelines to UIDAI immediately.
2. AUA / KUA shall ensure that the sub-AUAs, BCs and other sub-contractors are aware about Aadhaar Authentication related incident reporting.
3. AUA / KUA shall perform Root Cause Analysis (RCA) for major Aadhaar related incidents identified in its as well as its sub-contractors' ecosystem.
4. Any confidentiality breach/security breach of Aadhaar related information shall be reported to UIDAI within 24 hours.

2.13 Compliance

1. AUA / KUA shall comply with the UIDAI AUA / KUA agreement, Aadhaar Act 2016, Aadhaar Regulations 2016, as well as other notices and circulars published by UIDAI from time to time.
2. The AUA / KUA shall ensure that the application used for Aadhaar Authentication is audited by information system auditor(s) certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI. All Sub-AUAs shall also access authentication services only through duly audited client applications.
3. AUA shall take permission from UIDAI before appointment of an entity as their Sub-AUA. Also, the AUA shall take permission for already appointed Sub-AUAs.
4. AUA / KUA shall ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis to ensure compliance with UIDAI standards and specifications and the same shall be shared with UIDAI upon request.
5. In addition to the audits to be performed by AUA/KUA by itself on an annual basis, UIDAI may conduct audits of the operations and systems of AUA/KUA, either by itself or through an auditor appointed by UIDAI.
6. 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 the implementation of corrective and preventive action; and
   d. review the corrective action taken.
7. AUA/KUA shall use only licensed software for Aadhaar related infrastructure environment. Record of all software licenses shall be kept and updated regularly.
8. AUA/KUA and their ecosystem partners shall ensure compliance to all the relevant laws, regulations as well as other notices, circulars and guidelines as defined by UIDAI from time to time.
9. It is recommended that AUA / KUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analysing authentication related transactions to identify fraud.
10. AUA / KUA shall audit its Sub-AUAs, BCs or other sub-contractors providing Aadhaar Authentication services as per all the relevant laws, regulations as well as other notices, circulars and guidelines as defined by UIDAI from time to time.

11. For all authentication application deployed by an AUA/KUA and its Sub-AUA, the logo of an AUA/KUA should be clearly visible.

2.14 Data Protection

1. The AUA/KUA shall inform the resident of the following details by providing a notice at the time of authentication:
   a. the nature of information that will be shared by UIDAI upon authentication;
   b. the uses to which the information received during authentication may be put; and
   c. alternatives to submission of identity information.

   Further, AUA/KUA shall ensure that the information (as mentioned in para 2.15 (1)) is provided to the resident in local language as well. AUA/KUA shall make provisions for sharing the consent related information with visually/audibly challenged person in an appropriate manner.
2. AUA/KUA shall establish a data privacy policy addressing the privacy aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications. Such policy shall also be compliant to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Such policy shall be published on the website of AUA/KUA.
3. AUA/KUA shall obtain the consent of the resident for authentication in physical or preferably in electronic form and maintain logs or records of the consent obtained.
4. AUA/KUA shall maintain the logs of authentication transactions for a period of 2 (two) years during which period an Aadhaar number holder shall have the right to access such logs. Upon expiry of the 2 (two) year period, the logs shall be archived for a period of 5 (five) years or the number of years as required by the laws or regulations governing the entity, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by a court or required to be retained for any pending disputes.
5. The Aadhaar number holder may, at any time, revoke consent given to a KUA for storing his e-KYC data, received upon e-KYC authentication in encrypted form, or for sharing it with External Ecosystem Partner, and upon such revocation, the KUA shall delete the e-KYC data and cease any further processing.
6. AUA/KUA shall:
   a. report promptly to UIDAI (within 24 hours) any privacy incidents affecting the personal data of the residents; and
   b. extend full cooperation to UIDAI, or any agency appointed or authorised by UIDAI to cooperate while inquiries, incidents, claims and complaints are being handled in case of any security and privacy breach.
7. AUA/KUA upon termination of its services shall ensure the following:
   a. the arrangements for maintenance and preservation of authentication logs and other documents in accordance with the procedures as may be specified by UIDAI for this purpose;
   b. the arrangements for making authentication record available to the respective resident on such request;
   c. records of redressal of grievances, if any; and
   d. settlement of accounts with UIDAI, if any.

   Further, the obligations relating to authentication logs shall continue to remain in force despite termination of appointment.

2.15 Change Management

1. AUA/KUA shall document all changes to Aadhaar authentication applications, Infrastructure, processes and information processing facilities.
2. Change log/ register shall be maintained for all such changes performed.