Information Security Policy & Procedure for Aadhaar Usage by Backward Classes Welfare Department, Government of West Bengal (Sub-AUA under CDAC)

TermsandDefinitions

S.No.	Terms	Definitions
1	API	ApplicationProgramInterface
2	AUA/ASA	AuthenticationUserAgency/AuthenticationServiceAgency
3	BC	BusinessCorrespondent
4	Biometric Information	Photograph,fingerprint,irisscan,orsuchotherbiologicalattributes of an individual as may be specified by regulations
5	CA	Certifying Authority
6	CCTV	ClosedCircuit Television
7	CIDR	CentralIdentitiesData 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,recordsofentitlement,incomeormedical history
9	eKYC	ElectronicKnowYour User
10	GRC	Governance,Riskand 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. Peopleassets:UIDAIhumanresourcesand stakeholders e. Service assets: (logistics, building management systems, communications, utilities etc.)
12	HSM	HardwareSecurity Module
13	information/ informationasset	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,networkdetails etc.
14	IDS	IntrusionDetection System
15	IPS	IntrusionPrevention System
16	ISO	Informationsecurity division
17	ISO (ISO 27001)	InternationalOrganisationof Standardization
18	IT	Information Technology
19	KUA	Know your customer User Agencies
20	NDA	Non-Disclosure Agreement
21	NTP	NetworkTime 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	PersonalIdentity 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. Sexualorientation; f. Biometricdata; g. Geneticdata; h. Transgenderstatus; i. Intersexstatus; j. Casteortribe;or k. Religious orpoliticalbelief oraffiliation.
26	SOP	StandardOperatingProcedures
27	SPOC	SinglePointofContact
28	SSL	SecureSocketsLayer
29	STQC	Standardtestingandqualitycontrol
30	VA	VulnerabilityAssessment
31	VID	VirtualID
32	VPN	VirtualPrivateNetwork
33	WAF	WebApplicationFirewall

Information Security Domains and related Controls

A) Human Resources

1. Backward Classes Welfare Department, Government of West Bengal 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. Specific and specialised training shall be conducted for various functional roles involved in authentication ecosystem.
3. 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.

B) Asset Management

1. All assets used by the Backward Classes Welfare Department, Government of West Bengal (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. Backward Classes Welfare Department, Government of West Bengal 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. Backward Classes Welfare Department, Government of West Bengal 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. Backward Classes Welfare Department, Government of West Bengal shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets containing any Aadhaar related information.
7. Backward Classes Welfare Department, Government of West Bengal shall ensure that authentication devices used to capture resident's biometric are STQC certified registered devices. Backward Classes Welfare Department, Government of West Bengal 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 Backward Classes Welfare Department, Government of West Bengal and their sub-contractors for Aadhaar authentication shall be used after their hardening has been done as hardening baseline document. Government of West Bengal shall define their own hardening standards, unless specified by UIDAI.

C) 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 Backward Classes Welfare Department, Government of West Bengal.
2. Backward Classes Welfare Department, Government of West Bengal 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 Backward Classes Welfare Department, Government of West Bengal 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.

D) 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.

E) 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. 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.

5. The Backward Classes Welfare Department, Government of West Bengal 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. Global and local AUA shall make necessary changes in their authentication systems for use of Virtual token, UID token and Limited e-KYC.

F) Physical and Environmental Security

1. Backward Classes Welfare Department, Government of West Bengal servers should be placed in a secure cabinet in the Data Centre.
2. The Data Center hosting Aadhaar related information shall be fully secured, and access controlled.

G) Operations Security

1.Backward Classes Welfare Department, Government of West Bengalshall complete the Aadhaar AUA / KUA on-boarding process as defined by UIDAI, before the commencement of formal operations.
2. Backward Classes Welfare Department, Government of West Bengalshall 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.
3. Backward Classes Welfare Department, Government of West Bengalshall maintain the logs of the Aadhaar authentication transaction as defined in the Aadhaar (Authentication & Offline Verification) Regulations, 2021.
4. The Aadhaar authentication logs shall not, in any event, retain the PID information.
5. 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.
6. 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.
7. The client application used for Aadhaar authentication by Backward Classes Welfare Department, Government of West Bengaland its ecosystem partners should not store biometric data collected during authentication under any circumstances.
8. 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.
9. Backward Classes Welfare Department, Government of West Bengaland 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.
10. No data pertaining to the resident or the transaction shall be stored within the terminal device.
11. Aadhaar number and any other data kept in the Aadhaar Data Vault shall be kept in an encrypted format only.
12. 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.
13. Backward Classes Welfare Department, Government of West Bengalmay 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.
14.The user account shall be logged out after the session is finished.
15. An auto lock out mechanism for workstation, servers and/ or network device shall be implemented.

H) Application Security

1. Backward Classes Welfare Department, Government of West Bengal 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. Backward Classes Welfare Department, Government of West Bengal shall further ensure that there are no default passwords in use for the application framework or any components used by the application.

I) 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.

J) Information Security Incident Management

1. Backward Classes Welfare Department, Government of West Bengal shall be responsible for reporting any security weaknesses, incidents, possible misuse or violation of any of the stipulated guidelines to UIDAI immediately.
2. Backward Classes Welfare Department, Government of West Bengal shall ensure that the sub-contractors are aware about Aadhaar Authentication related incident reporting.
3. Backward Classes Welfare Department, Government of West Bengal 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.

K) Compliance

1. Backward Classes Welfare Department, Government of West Bengal 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. Backward Classes Welfare Department, Government of West Bengal 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. Backward Classes Welfare Department, Government of West Bengal 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.
4. 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.
5..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.
6. Backward Classes Welfare Department, Government of West Bengal shall use only licensed software for Aadhaar related infrastructure environment. Record of all software licenses shall be kept and updated regularly.
7. Backward Classes Welfare Department, Government of West Bengal 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.
8. 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.

L) Data Protection

1. Backward Classes Welfare Department, Government of West Bengal 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

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. Backward Classes Welfare Department, Government of West Bengal 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.
3. Backward Classes Welfare Department, Government of West Bengal 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.
4. 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.
5.Backward Classes Welfare Department, Government of West Bengal 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.
6.Backward Classes Welfare Department, Government of West Bengal 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.

M) Change Management

1. Backward Classes Welfare Department, Government of West Bengal 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

Secretary
Backward Classes Welfare Department
Government of West Bengal