AUA/KUA INFORMATION SECURITY POLICY

Department of IT & Electronics,
Government of West Bengal

TABLE OF CONTENTS

VERSION HISTORY

Version	Review cycle	Reviewed by	Approved by
V1.0	Aug 2023 – Dec 2023	Joint Secretary, DoIT&E, GoWB	Chief Information Security Officer (CISO), GoWB
V2.0	Jan 2024 – Mar2024	Joint Secretary, DoIT&E, GoWB	Chief Information Security Officer (CISO), GoWB
V3.0	Apr 2024 – Jun 2024	Joint Secretary, DoIT&E, GoWB	Chief Information Security Officer (CISO), GoWB
V4.0	Jul 2024 – Sep 2024	Joint Secretary, DoIT&E, GoWB	Chief Information Security Officer (CISO), GoWB

PREFACE

"Data is the new oil" - Clive Humby

In an era where information flows seamlessly through the digital arteries of our interconnected world, data has become a cornerstone of modern life. It permeates every facet of our existence, from personal communication to business operations, scientific advancements to political decision-making and policy making. Data is the lifeblood of the digital age, and its significance cannot be overstated.

Data can be defined as any discrete and objective pieces of information. It encompasses a wide array of forms, such as text, numbers, images, audio, and video, which collectively fuel our digital interactions. Data can be categorized into two main types: structured data, which is highly organized and easily processed, and unstructured data, which is more complex and requires advanced techniques for analysis.

As our reliance on data continues to grow, so does the paramount concern for data privacy. Data privacy refers to the protection of individuals' personal information and the control they have over its collection, storage, and dissemination. It is the fundamental concept that ensures our right to keep sensitive data out of the wrong hands. This includes not only personal details like names and addresses but also the patterns of our online behavior, our financial information, and even our health records.

In today's digital landscape, the need for data privacy has been more critical than ever before. With the proliferation of data-driven technologies, there is a constant exchange of data between individuals, businesses, and governments. This exchange, however, brings with it the potential for misuse and abuse of personal information. The consequences of data breaches and privacy violations can be dire, ranging from identity theft to erosion of trust in institutions.

Hence, the importance of this document lies in its exploration of data privacy – to empower individuals, government bodies and organizations to protect sensitive information and build trust in our increasingly data-centric world. Understanding the nuances of data privacy, its regulations, and best practices is a crucial step in navigating the complex landscape of our digital age. By shedding light on these aspects, we aim to contribute to the ongoing discourse on safeguarding our digital identities, fostering responsible data handling, and advocating for the rights of data subjects.

This document, therefore, serves as a valuable resource to demystify the world of data privacy and empower individuals, government bodies and organizations to take charge of their data in a responsible and ethical manner. Through knowledge and informed action, we can collectively ensure that data remains a force for good, benefitting society while respecting the fundamental right to privacy.

PRINCIPLES OF DATA PRIVACY

PRINCIPLE 01

The principle of consented, lawful and transparent use of personal data

PRINCIPLE 02

The principle of purpose limitation (use of personal data only for the purpose specified at the time of obtaining consent of the Data Principal).

PRINCIPLE 03

The principle of data minimization (collection of only as much personal data as is necessary to serve the specified purpose).

PRINCIPLE 04

The principle of data accuracy (ensuring data is correct and updated).

PRINCIPLE 05

The principle of storage limitation (storing data only till it is needed for the specified purpose).

PRINCIPLE 06

The principle of reasonable security safeguards.

PRINCIPLE 07

The principle of accountability through adjudication of data breaches.

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

STAKEHOLDERS IN WORLD OF DATA PRIVACY

DATA PRINCIPALS

Individuals or organizations whose personal data is being processed.

In essence: Owner of the data

Who can be Data Principals?

- ✓ Individual citizens
- ✓ Organizations
- ✓ Government & Government bodies

DATA FIDUCIARY

Anyone deciding what data will be collected, how it will be collected and the purpose of its use.

Who can be Data Fiduciary?

- ✓ Organizations
- ✓ Government & Government bodies

CONSENT

Give explicit permission for manage, review and use personal data

Who can give consent?
Individual citizens, organizations, Government & Government bodies whose data will be used by data fiduciary.

CONSENT MANAGER

Anyone who assists Data Principals and Data Fiduciaries to give, manage, review and withdraw consent

Who can be Consent Manager?

Person registered with Data Protection Board

DATA PROCESSOR

Anyone who processes data on behalf of Data Fiduciaries based on their instructions.

Who can be Data Processor?

- ✓ Organizations
- ✓ Government & Government bodies

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

DIGITAL PERSONAL DATA EXPLAINED

Digital personal data encompasses a wide range of information in a digital format that can identify an individual. This includes basic identifiers, online profiles, financial and health information, employment details, online behavior, geolocation data, communication records, and more.

- Basic Identifiers: A person's name, date of birth, physical address, email address, and phone number
- Online Identifiers: Usernames, social media profiles, IP addresses, and device IDs
- Biographical Information: Gender, nationality, and marital status
- Financial Details: Bank account numbers, credit card information, and financial transaction records
- Health and Medical Information: Medical records, health insurance details, and health-related app data
- Employment Information: Job titles, workplace, and salary details
- Digital Behavior and Preferences like Data related to an individual's online activities, search history, purchase history, and preferences in websites, apps, or products
- Social and Relationships: Data about an individual's family, friends, and social connections
- Geolocation Data: Information that can reveal an individual's location through GPS or other tracking technologies
- Communication Data: Emails, messages, and call logs

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

ABOUT CONSENT

What is consent?

Consent means a person's voluntary agreement to let an organization or individual or government collect and use their personal data for specific purposes. This agreement must be freely given, informed, specific, reversible, and documented, and it has special rules for children's data.

Consent should be specific to each data processing activity. It should not be bundled together with unrelated purposes, and individuals should have a clear understanding of what they are consenting to. Ambiguous or overly broad consent is not considered valid.

Why is consent important?

- ✓ Empowers individual control by allowing people or organization or government to decide how their personal data is used
- ✓ Ensures compliance required by data privacy laws and regulations
- ✓ Promotes transparency by encouraging clear and open communication between data controllers and data principals and minimizes unnecessary data collection
- ✓ Upholds ethical data handling by encouraging fair and respectful treatment of personal data

How to give consent?

- ✓ The consent should be established through a clear affirmative action by the Data Principal
- ✓ When processing a minor's personal data, consent from their legal guardian needs to be taken
- ✓ Data Principals have the authority to withdraw their consent at any point during the processing

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

INFORMED DECISION MAKING

It is important for the Data Principals to make an informed decision pertaining to sharing their data, the purpose of the data use, duration and so on. A privacy notice is a document that informs the data principals about how their personal data will be collected and used by an organization or government or any entity. Its importance lies in promoting transparency, enabling informed consent, complying with legal requirements, empowering data principals to exercise their data rights, demonstrating accountability, and mitigating legal and financial risks for the organization or government or individual (both data principal & data fiduciary).

Q. Who is responsible to furnish privacy notice while data collection?

A. Data Fiduciary

Q. Who will provide response to privacy notice?

A. Data Principal

Q. Should the privacy notice have details of filling a complaint in case it is required?

A. Yes

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

DOS & DON'TS OF DATA FIDUCIARIES

- ✓ Implement technical and organizational security safeguard measures to safeguard personal data
- ✓ Determine legal ground of processing and obtain consent from Data Principals where required
- ✓ Provide a privacy notice while obtaining consent from Data Principals
- ✓ Implement a mechanism for Data Principals to exercise their rights
- ✓ Implement a grievance redressal mechanism for handling queries from Data Principals and have an officer (Data Protection Officer) to respond to queries from Data Principals
- ✓ Sign a valid contract with Data Processors to ensure key obligations are abided by them, including timely deletion of data
- ✓ Data Fiduciaries have a responsibility to irrecoverably delete personal data once the purpose for its collection is achieved
- ✓ Data Fiduciaries have a responsibility to irrecoverably delete personal data when the Data Principal withdraws their consent
- ✓ Data Fiduciary is required to inform the Data Protection Board and the Data Principals regarding data breaches

In addition to above, **a Significant Data Fiduciary** (Organization or Government that processes large volume of sensitive data) must also

- ✓ Appoint a Data Protection Officer based in India
- ✓ Appoint an independent data auditor and conduct periodic data audits
- ✓ Conduct Data Protection Impact Assessment periodically

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

DOS & DON'TS OF DATA PRINCIPAL

- ✓ Data Principals are entitled to access information related to the processing of their data, encompassing the categories of personal data shared and the identities of all Data Processors with whom their personal data has been shared
- ✓ Data Principals possess the authority to halt data processing by revoking their consent through Consent Manager
- ✓ Data Principals can request Data Fiduciaries to rectify, supplement, update, or delete their personal data
- ✓ Data Principals retain the right to seek redressal for their grievances. Data Fiduciaries and Consent Managers must designate qualified individuals (Data Protection Officer, if required) to handle these grievances
- ✓ In the event of incapacity or the demise of the Data Principal, they may designate or nominate a representative to exercise their rights on their behalf

In case of processing personal data of children and individuals with disabilities it is mandatory to obtain consent from their legal guardians

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

DATA RETENTION

Data retention is the practice of preserving data for a specific period to meet technical, business, or regulatory requirements. The data should be retained as per data retention schedule which is varied depending upon:

- Criticality level of case
- The purpose of data use and retention
- The nature or type of data in consideration – business or personal or public data
- Legality of the department or organization collecting, processing, and retaining data

How to follow data retention to abide by data privacy guidelines?

- ✓ Data Fiduciary shall itself or direct the Data Processor, to erase personal data as soon as the Data Principal withdraws consent or the purpose of data use is achieved whichever is earlier, unless retention is necessary for compliance with any law

Based on international standard practices, data retention period for different types of data will be as follows:

CATEGORY	RETENTION PERIOD (Data Centre & DR site)	TOTAL RETENTION PERIOD (Including archival)
Medical Records	3 years	25 years (inclusive of the 3 years) Or based on applicable regulations
HR Records	3 years	25 years (inclusive of the 3 years) Or based on applicable regulations
Medical & Security Assistance Case Records	2 years	3 years (inclusive of the 2 years)
Call Recordings	1 year	2 years
Audit logs	3 months	2 years
Corporate Secretariate Record	Life of the entity	Life of the entity + 50 years
Accounting & Financial Records	2 years	7 years or based on applicable regulations
Procurement & Contract Record	Contract Duration	Contract duration + 7 years or based on applicable regulations
Travel Tracker Records	2 years or based on contractual commitments	3 years or based on contractual commitments
Other Records	2 years or based on applicable regulations	2 years or based on applicable regulations
Logs of Aadhaar authentication transaction for audit	2 years or based on applicable regulations	5 years or based on applicable regulations

Refer "West Bengal State Electronic Data Centre Storage Sharing and Electronic Data Retention Guidelines, 2020" for details.

STEPS TO ENSURE DATA ANONYMIZATION AND ADHERE TO DATA PRIVACY

- ✓ Data fiduciaries should ensure that an individual cannot be re-identified from their anonymized data
- ✓ Data fiduciaries should instruct the Data Processors and ensure that personal data is shared only in anonymized form
- ✓ Data fiduciaries should make strategies considering different industries and sectors having varied arrangements and models that can be used for sharing anonymized data

Refer "West Bengal State Public Transactional Data Sharing Guidelines, 2020" for details.

EXEMPTIONS

There are certain scenarios under which Data Principals do not possess the right to request erasure, correction, access to their personal data, or withdraw their consent. The scenarios are given below:

SCENARIO 01

For notified agencies, in the interest of security, sovereignty, public order, etc

SCENARIO 02

For research, archiving or statistical purposes

SCENARIO 03

For medical emergencies, employment

SCENARIO 04

To enforce legal rights and claims

SCENARIO 05

To perform judicial or regulatory functions

SCENARIO 06

To prevent, detect, investigate or prosecute offences

SCENARIO 07

To process personal data of non-residents under foreign contract in India

SCENARIO 08

For approved merger, demerger etc

SCENARIO 09

To locate defaulters and their financial assets etc

Reference: Digital Personal Data Protection Act 2023
Decoding Digital Personal Data Protection Act 2023 by KPMG

RESOURCE CREATION AND CAPACITY BUILDING

RESOURCE CREATION

The Organizations or Government Bodies which will be designated as Significant Data Fiduciary should appoint a **Data Protection Officer** and an independent data auditor **(Data Protection Auditor)**.

CAPACITY BUILDING

To increase awareness and skills among the employees of the Government and other Organizations, it is required to conduct periodic training to sensitize them about their rights and duties and guidelines to prevent risk of being susceptible to breaches.

The training should encompass:

- ✓ General awareness programs for all employees to foster a culture of data privacy
- ✓ Specific departments, such as IT and Legal, will be trained on specialized modules of data privacy rules and their implementation
- ✓ Mandatory training topics including data security best practices, understanding and compliance with data privacy regulations, recognizing and responding to data breaches, and safeguarding personal and confidential information

INFORMATION SECURITY DOMAINS AND RELATED CONTROLS

Human Resources

- AUA/KUA shall appoint a SPOC/team for Aadhaar related activities and communication with UIDAI
- AUA/KUA 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.
- Induction as well as periodic functional and information security trainings shall be conducted for all AUA/KUA personnel for Aadhaar related authentication services. The training shall include all relevant security guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016 and all circulars/notices published from time to time.
- All employees accessing UIDAI Information Assets shall be made aware of UIDAI information security policy and controls.
- 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.
- AUA / KUA shall ensure that the sub-AUAs, BCs and other sub-contractors are aware about Aadhaar Authentication related incident reporting.

Asset Management

- All Assets used by the AUA/KUA for the purpose of delivering services to residents using Aadhaar authentication services shall be identified, labelled and classified. Details of the Information Assets shall be recorded.
- The assets which are scheduled to be disposed shall be disposed as per AUA/KUA's Information Security Policy. Information systems / documents containing Aadhaar related information shall be disposed-off securely.
- Before sending any equipment out for repair, the equipment shall be sanitized to ensure that it does not contain any UIDAI sensitive data.
- AUA / KUA and its Sub-AUAs shall not transfer or make an unauthorized copy of any identity information from removable media to any personal device or other unauthorized electronic media / storage devices.
- AUA and its Sub-AUAs shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.
- Authentication devices used to capture residents' biometric shall be STQC certified as specified by UIDAI.
- AUA/KUA should carry out analysis of devices with high failure rates and replace them. Defective biometric devices should be replaced and the defective devices should be destroyed as E-waste.

- Annual review & assessment of systems, infrastructure, etc shall be conducted by a CERT-In empaneled agency to ensure compliance with Aadhaar Act, Regulations and specifications. 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;

d) Review the corrective action taken

Access Control

- 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 UIDAI information;
- AUA/KUA employees with access to UIDAI information assets shall:
    - Have least privilege access for information access and processing;
    - The operator must be logged out after the session is finished.
    - Implement an equipment locking mechanism for workstation, servers and/ or network device
- The application should have auto log out feature i.e. after a certain time of inactivity (15 mins or as specified in the UIDAI Authentication Regulations document), the application should logout.
- Access rights and privileges to information processing facilities 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
- 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;
- Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approved and documented where there is no alternative;
- 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 similar password vault must be used to maintain the access log register.

- 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.
- 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.
- The local security settings on all the systems shall be aligned and synced with the Active Directory or similar solutions for local policy enforcement.
- If the application is operator assisted, the operator shall first confirm his identity by authenticating himself before authenticating the residents.
- The access rules of firewalls shall be maintained only by users responsible for firewall administration.
- 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.
- AUA/KUA should inform UIDAI without delay within 72 hours after having knowledge of misuse of any information related to the Aadhaar related information or system, compromise of Aadhaar related information. Entity should ensure to comply with Regulation 14A(d) Of Aadhaar (Authentication and offline verification) Regulations, 2021.
- AUA/KUA should implement process and procedure to perform periodic information security risk assessment on its third-party having access to Aadhaar application and resident data.

Password Policy

- The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login;
- All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner;
- Keeping a paper record of passwords shall be avoided, unless this can be stored securely;

- If the passwords are being stored in the database or any other form, they should be stored in encrypted form.
- Passwords shall be changed whenever there is any indication of possible system or password compromise;
- Complex passwords shall be selected, with a minimum length of eight characters and should ensure—
    a. are not based on anything somebody else may easily guess or obtain using person related information, e.g., name, telephone number and date of birth;
    b. is free of consecutive identical characters or all-numeric or all-alphabetical groups;
    c. contain at least one numeric, one uppercase letter, one lowercase letter and one special character;
    d. are required to be changed at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords);
    e. do not allow the use of the last five passwords;
    f. do not allow the username and password to be the same for a particular user; and
    g. do not use the same password for various UIDAI access needs of a particular user.
- Passwords shall not be hardcoded in codes, login scripts, any executable program or files;
- Password should not be stored or transmitted in applications in clear text or in any reversible form.
- Passwords shall not be included in any automated log-on process, e.g. stored in a macro or function key;

Cryptography

- The Personal Identity data (PID) block comprising of the resident's demographic / /biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication.
- The PID shall be encrypted during transit and flow within the AUA ecosystem and while sharing this information with ASAs; Logs of the authentication transactions shall be maintained but PID
- The encrypted PID block should 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;
- The authentication request shall be digitally signed by AUA/KUA

- While establishing a secure channel to the AADHAAR Authentication Server (AAS), the AUA/KUA 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 or 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);
- Key management activities shall be performed by AUA/KUA to protect the keys throughout their lifecycle. The activities shall address the following aspects of key management, including;
    - key generation;
    - key distribution;
    - Secure key storage;
    - key custodians and requirements for dual Control;
    - prevention of unauthorized substitution of keys;
    - Replacement of known or suspected compromised keys;
    - Key revocation and logging and auditing of key management related activities.

Data protection

- AUA/KUA should establish a data protection policy addressing, inter alia, data protection related aspects under—
    a. the Aadhaar Act, the regulations made thereunder and the standards and specifications issued by UIDAI from time to time;
    b. the Information Technology Act, 2000 ("IT Act"); and
    c. till the coming into force of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") and, on and from the date of coming into force of the DPDP Act, the said Act and the rules made thereunder.

Such policy should be published on the website of AUA/KUA and the URL for the same should be mentioned.

Operations Security

- AUA/KUA shall complete the AADHAAR AUA on-boarding process before the commencement of formal operations;
- 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 failure;
- Persons 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;
- 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;
- The Test and Production facilities/ environments must be physically and/or logically separated.

- The Operating System as well as the network services used for communication shall be updated with the latest security patches.
- 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;
- Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
- AUA/KUA 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;
- All hosts that connect to the AADHAAR Authentication Service information shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed on such hosts;
- AUA/KUA shall ensure that the event logs are to be recorded and stored to assist in future investigations and access control monitoring.
- AUA/KUA should ensure that the operations and systems of its Sub-AUAs and Sub-KUAs are audited on an annual basis by an information systems auditor certified by a recognized body, to ensure compliance with such standards and specifications as UIDAI may specify from time to time and that the audit report is shared with UIDAI.

- 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;
- The authentication audit logs should contain, but not limited to, the following transactional details:
    - Aadhaar Number against which authentication is sought;
    - Specified parameters of authentication request submitted;
    - Specified parameters received as authentication response;
    - The record of disclosure of information to the Aadhaar number holder at the time of authentication
    - Record of the consent of Aadhaar number holder for the resident
    - Details of the authentication transaction such as API Name ,AUA /KUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-identity information.
- Network intrusion and prevention systems should be in place;
- Logs shall not, in any event, retain the PID, biometric and OTP information;
- The logs of authentication transactions shall be maintained by AUA/KUA 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;
- 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 of Govt. of WB, 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;
- 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;
- The AUA server host shall reside in a segregated network segment that is isolated from the rest of the network of the AUA/KUA; The AUA server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities;

Intellectual Property

- AUA is aware that UIDAI holds the copyright for the Aadhaar logo and understands that any unauthorized reproduction of the same constitutes infringement of UIDAI's rights therein and may render the person so unauthorizedly reproducing it liable under civil and criminal laws.
- It is hereby mutually agreed between the Parties that all rights (including intellectual property rights), title and interests in the use of the Aadhaar logo shall, at any time, during the period of the Agreement and thereafter, vests in UIDAI and that the AUA shall only have a non-exclusive right to use the same during such period.
- The AUA hereby unequivocally agrees that—
  a. it shall use the Aadhaar logo without modifying it in any manner;
  b. it shall use the Aadhaar logo only during the period of the Agreement and for promotional, educational and informational purposes related to the use of UIDAI's Authentication facilities;
  c. it shall not authorize any other entity or person to use the Aadhaar logo, except with the prior permission in writing from UIDAI and in accordance with such terms and conditions as UIDAI may specify;
  d. on becoming aware of any unauthorized use, copy, infringement or misuse of the Aadhaar logo, it shall forthwith inform UIDAI, in writing, of the same and, in case UIDAI so requires, the AUA shall itself initiate legal action or proceedings, or join in or cooperate in such action or proceedings, and execute such documents and do such things as may reasonably be necessary to protect the rights, title and interests of UIDAI; and
  e. any breach in adherence to the preceding sub-clauses shall constitute a material breach of this Agreement.

Communications security

- In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometric reader and the device performing the encryption shall be secured against all security threats / attacks

- Terminal devices shall provide different logins for operators. These users shall be authenticated using some additional authentication scheme such as passwords, AADHAAR authentication, etc.

- Each terminal shall have a unique terminal ID. This number must be transmitted with each transaction along with UIDAI assigned institution code for the AUA as specified by the latest UIDAI API documents

- A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transaction processed;

- The network between AUA ASA shall be secured. AUA 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.

- The AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA server from all sources;

- Special consideration shall be given to Wireless networks due to poorly defined network perimeter. Appropriate authentication, encryption and user level network access control technologies shall be implemented to secure access to the network

- 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;

- UIDAI should be informed about the ASAs, the AUA has entered into an agreement;

Information Security Incident Management

- AUA/KUA shall be responsible for reporting any security weaknesses, any incidents, possible, misuse, or violation of any of the stipulated guidelines to UIDAI immediately.
- AUA/KUA should—
  a. inform UIDAI misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within its network, and report any confidentiality security breach of Aadhaar related information to UIDAI within 24 hours;
  b. report cyber incidents as mentioned in Annexure I to the directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022-CERT-In, within 6 hours of noticing such incidents or the same being brought to their notice; and
  c. on and from the date of coming into force of sub-section (6) of section 8 of the DPDP Act, intimation of personal data breach to the Board and each affected Data Principal, within such time as may be prescribed by rules made under the said Act.

Cookies

A cookie is a piece of software code that an Internet website sends to your browser when you access information in that site. This site does not use cookies.

API whitelisting and API gateway implementation

AUA/KUA should ensure that it is using the latest API version and that it has API whitelist implemented to limit the data exchange using only authorized APIs and with whitelisted IP addresses. AUA/KUA should also ensure that API gateway is deployed for centralized security enforcement, monitoring and management. AUA/KUA should ensure that rate limitation and throttling mechanisms are implemented to prevent abuse of API and Distributed Denial of Service (DDoS) attacks. AUA/KUA should ensure that Cross-Origin Resource Sharing (CORS) parameters are configured to restrict unauthorized domains from accessing APIs from the client side.

E-mail Management

E-mail address will only be recorded if you choose to send a message. It will only be used for the purpose for which you have provided it and will not be added to a mailing list. Your e-mail address will not be used for any other purpose, and will not be disclosed without your consent.

Collection of Personal Information

If you are asked for any other Personal Information you will be informed how it will be used if you choose to give it. If at any time you believe the principles referred to in this privacy statement have not been followed, or have any other comments on these principles, please notify the Web Information Manager by sending email to itewb@wb.gov.in

Note: The use of the term 'Personal Information' in this privacy statement refers to any information from which your identity is apparent or can be reasonably ascertained.

Reasonable Security Practices

Reasonable security measures such as administrative, technical, operational and physical controls have been implemented to ensure the security of personal information, if collected.

The policy shall align with and abide by any new or amended directives, guidelines, terms and conditions, circulars, notifications, and standards, et cetera, as may be stipulated by the Unique Identification Authority of India (UIDAI) from time to time. This policy shall remain in force until such a juncture that a revised policy is promulgated.

Mandatory Compliances to be adhered to

I. AUA/KUA should comply with the Aadhaar Act, 2016.
II. AUA/KUA should comply with Aadhaar (Authentication and Offline Verification) Regulations, 2021
III. AUA/KUA should comply with Aadhaar (Data Security) Regulations, 2016.

IV. AUA/KUA should comply with Aadhaar (Sharing of Information) Regulations, 2016.

V. AUA/KUA should comply with UIDAI Information Security policy in respect to Entity available in the compendium on UIDAI official website.

VI. AUA/KUA should comply with Aadhaar Do's and Don'ts available in the compendium on UIDAI official website.

VII. AUA/KUA should comply all the requirements of UIDAI letter HQ- 13023/1/2020-AUTH-1-HQ/2084 dated 20 June 2022 (Removal of Old and deployed devices from Authentication ecosystem for strengthening authentication security)

VIII. AUA/KUA should always comply with provisions of AUA / KUA Agreement with UIDAI.

IX. AUA/KUA should comply with all the requirements of UIDAI circular K 11022/460/2016-UIDAI (Auth-II) dated 6 July 2017 (Appointment of Sub-AUA – Application & Undertaking)

X. AUA/KUA should comply with all the requirements of UIDAI circular K-11022/631/2017-UIDAI (Auth-II) dated 27 November 2017 (Sharing of e-KYC data with their Sub-AUAs).

XI. AUA/KUA should comply with all the requirements of UIDAI circular K-11020/217/2018-UIDAI (Auth-I) dated 10 January 2018 (Implementation of Virtual ID, UID Token and Limited KYC).

XII. AUA/KUA should comply with all the requirements of UIDAI Circular No. 04 of 2018, K-11020/217/2018-UIDAI (Auth-I), dated 1st May 2018 (Implementation of Virtual ID, UID Token and Limited KYC).

XIII. AUA/KUA should comply with all the requirements of UIDAI Circular No. 05 of 2018, K-11020/217/2018-UIDAI (Auth-I), dated 16th May 2018 (Classification of Global AUAs and Local AUAs).

XIV. AUA/KUA should comply with all the requirements of UIDAI Circular No. 06 of 2018, K-11020/217/2018-UIDAI (Auth-I), dated 04th June 2018 (Implementation of Virtual ID, UID Token and Limited KYC).

XV. The AUAs should comply with Regulation number 15, Chapter-III, Aadhaar (Authentication) Regulations, 2016 Further clarified by: 1. UIDAI Circular No. F.No.K 11022/460/2016-UIDAI (Auth-II), dated 28 February 2017 2. UIDAI Circular No. F.No.K 11022/460/2016-UIDAI (Auth-II), dated 06 July 2017

XVI. The KUAs should comply with Regulation number 16, Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021

XVII. AUA/KUA should comply with Regulation number 22, Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021

XVIII. AUA/KUA should comply with all relevant laws, rules and regulations, including, but not limited to, Aadhaar Act, 2016 and its Regulations, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.

XIX. AUA/KUA should comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016

Special Secretary
Information Technology & Electronics Dept.
Government of West Bengal

Contact Us

If you have any questions or concerns about this privacy policy or our treatment of your personal information, please contact us by e-mail at itewb@wb.gov.in, or by mail using the details provided below:

Department of Information Technology & Electronics
Government of West Bengal
Monibhandar (5th and 6th floor)
Premise of Webel Bhavan
Block - EP & GP, Sector-V, Saltlake City
Kolkata - 700 091
Phone: 91-33 2357-6454
Email: itewb@wb.gov.in
Call: +91-6292234484

Special Secretary
Information Technology & Electronics Deptt.
Government of West Bengal

ADG & IGP, Cyber Cell
West Bengal