Aadhaar Information Security and Privacy Policy Document

Prepared for Government of Himachal Pradesh

Created By Department of Digital Technologies & Governance (DDT&G)

Contents

1. Purpose

This policy establishes the Information Security Framework for the Department of Digital Technologies and Governance (DDT&G), Government of Himachal Pradesh — an authorized Authentication User Agency (AUA) / KYC User Agency (KUA) under the Unique Identification Authority of India (UIDAI) — including all empanelled Sub-AUAs and Sub-KUAs.

The policy defines the mandatory controls, requirements, identity and access controls, and best practices necessary to ensure secure access, processing, transmission, storage, and management of Aadhaar authentication data, in strict compliance with:

- The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
- Aadhaar Regulations, 2016
- UIDAI guidelines, circulars and advisories issued from time to time

This policy applies to all stakeholders involved in Aadhaar authentication and e-KYC operations and establishes uniform Information Security standards for AUAs/Sub-AUAs and KUAs/Sub-KUAs.

2. Scope

This policy applies to all systems, personnel, vendors, processes, and environments involved in Aadhaar authentication and Aadhaar-related application development or operations handled by DDT&G and its Sub-AUAs/Sub-KUAs.

It governs protection of:

- Confidentiality, Integrity and Availability (CIA) of Aadhaar data
- Secure collection, processing and transmission of Aadhaar-related information
- Storage and management of logs and authentication records
- Compliance obligations of AUA/KUA ecosystem partners

As an authorized AUA/KUA, the Department may provide Aadhaar-based authentication services directly or through approved Sub-AUAs, strictly for permitted purposes and with informed consent.

A Privacy Policy forms an integral part of this framework to ensure robust protection of beneficiary personal information and adherence to UIDAI-mandated privacy principles.

3. Key Definitions

AUA (Authentication User Agency)
Organization authorized by UIDAI to perform Aadhaar authentication services.

Sub-AUA
Entity authorized to perform Aadhaar authentication through a parent AUA, without direct access to UIDAI authentication services.

ASA (Authentication Service Agency)
Entity providing secure connectivity between AUAs and the UIDAI Central Identities Data Repository (CIDR).

CIDR
Central Identities Data Repository — UIDAI's database storing Aadhaar biometric and demographic information.

CISO
Chief Information Security Officer — responsible for cybersecurity governance and compliance.

API
Application Programming Interface enabling secure system-to-system communication.

KUA (KYC User Agency)
Entity authorized to perform Aadhaar-based KYC services.

Assets (classified as):

1. **Paper Assets** – policies, manuals, records
2. **Physical Assets** – IT equipment, devices, infrastructure
3. **Software Assets** – applications, databases, tools
4. **Human Assets** – employees and authorized stakeholders
5. **Service Assets** – utilities, logistics, communication services

VPN
Secure encrypted network channel.

NDA
Non-Disclosure Agreement to protect confidential information.

NTP
Protocol for clock synchronization across systems.

OTP
One-Time Password used for secure authentication.

PID (Personally Identifiable Data)
Any data capable of identifying an individual.

SPOC
Designated Single Point of Contact for UIDAI coordination.

STQC
Government agency providing IT quality assurance and certification.

SSL
Secure protocol ensuring encrypted communication.

VA (Vulnerability Assessment)
Process to identify and mitigate security weaknesses.

AAS
Aadhaar Authentication Server operated by UIDAI.

TPOC
Technical Point of Contact.

---

4. Information Security Domains and Controls

4.1 Human Resources

a) Vendors/third parties shall appoint a SPOC/team for Aadhaar operations.
b) Background verification must be completed before deployment. NDAs are mandatory.
c) Aadhaar data accessed during work shall remain strictly confidential
d) Mandatory induction and periodic security training shall be conducted.
e) All users handling UIDAI assets shall be aware of applicable policies and controls.

4.2 Asset Management

a) All AUA/KUA/Sub-AUA assets shall be identified, classified, labelled and documented.
b) Assets marked for disposal shall be securely destroyed.
c) Equipment sent for repair shall be sanitized first.
d) Unauthorized copying or transfer of Aadhaar data is prohibited.
e) Only STQC-certified biometric devices shall be used.
f) Controls shall exist to prevent loss, theft or misuse of assets.
g) Disposal processes must follow Information Security Policy guidelines.

4.3 Access Control

a) Only authorized personnel may access Aadhaar-related systems.

b) Least-privilege access shall be enforced.

c) Access shall be revoked within 24 hours upon separation.

d) Group/shared IDs are prohibited.

e) Administrative passwords must be securely stored (vault/fireproof safe).

f) Operators must authenticate themselves before processing resident authentication.

4.4 Password Policy

a) Initial passwords must be changed on first login.

b) Accounts lock after 3 failed attempts.

c) Minimum password length: **14 characters**

d) Must contain uppercase, lowercase, numeric and special characters.

e) Must not be reused (last 5 passwords restricted).

f) Passwords must not be stored, displayed, shared, or hard-coded.

g) Compromised passwords must be reported and changed immediately.

4.5 Cryptography

a) The personal Identify data (PID) shall always be encrypted during transmission and within the AUA ecosystem.

b) Authentication logs shall not contain decrypted PID.

c) Authentication requests must be digitally signed.

d) Secure channel with Aadhaar Authentication Server (AAS) must verify:

- CA-signed certificate
- Validity and non-revocation
- Correct Common name (CN) mapping to domain
- Key management must address:

Generation, distribution, storage, custodianship, dual control, rotation and substitution prevention.

4.6 Operational Security

a) AUA onboarding must be completed before operations.

b) SOPs must exist for operations, monitoring and incident handling.

c) Segregation of duties is mandatory.

d) Test and production environments shall be isolated.

e) Patch management must be formally implemented.

f) Regular vulnerability (VA) exercises are mandatory.

g) Antivirus and endpoint security must be installed.

h) Logs shall be recorded, monitored and retained as mandated.

i) Intrusion Prevention/Detection Systems must be deployed.

j) AUA logs must be retained, archived, and deleted per UIDAI retention timelines.

k) All system clocks must sync via authorized NTP server.

l) AUA servers shall operate only within segregated network segments.

m) Sub-AUAs shall submit requests to AUA, no request shall be routed directly from the application to the AUA.

n) TPOC to make sure UIDAI policies/guidelines are being followed while implementing the solution.

4.7 Data Security

a) Aadhaar numbers must be collected and transmitted only through secure, UIDAI-approved channels.

b) Biometric data shall be captured only through registered devices.

c) OTP data must be encrypted before transmission.

d) PID shall never be stored by AUAs/Sub-AUAs.

e) e-KYC information must be stored only in encrypted form.

f) Local AUAs shall not store Aadhaar numbers.

g) Global AUAs shall store Aadhaar numbers only in the Aadhaar Data Vault.

h) Cryptographic keys must reside only in HSMs.

i) Only certified biometric devices shall be used.

j) All authentication/e-KYC applications must undergo compliance testing and annual audits.

---

5. Compliance and Enforcement

All personnel, vendors, Sub-AUAs/Sub-KUAs must strictly adhere to this policy. Any violation may result in:

- Suspension of access
- Termination of authorization
- Disciplinary and legal action as applicable

---

6. Review and Updates

This policy shall be reviewed if required due to regulatory or technological changes, and updated as per UIDAI guidelines.

Approved vide NN: 81
Secretary to the
Government of Himachal Pradesh

File No: SITEG-F05(12)/6/2025-IT-DDTG (e-298076)-145 **Dated:** 13-7-2026

Copy forwarded for information & Necessary action to:

1. All the Administrative Secretaries to the Government of Himachal Pradesh.
2. All the Heads of the Departments in Himachal Pradesh.
3. The Deputy Director General, UIDAI, Regional Office, SCO-95-98, Sector-17B Chandigarh.
4. The Divisional Commissioner, Shimla, Kangra and Mandi.
5. All the Deputy Commissioners in Himachal Pradesh.
6. All the Superintendent of Police in Himachal Pradesh.
7. All the Managing Director/Member Secretary/ Commissioner Secretary/ Chief Executive Officer/ Registrars of Boards/Corporations/Councils/Authority/ Universities/Municipal Corporations/ Co-perative Banks in Himachal Pradesh.
8. Guard File.

Director,
Department of Digital Technologies and Governance,
Himachal Pradesh