GOVERNMENT OF RAJASTHAN
Department of Information Technology & Communication
IT Building, Yojana Bhawan Campus, Tilak Marg, C-Scheme, Jaipur-302005,
Website: www.doitc.rajasthan.gov.in

Ref. No: F11(76)/DoIT&C/2022/Vol-3-00145 **Dated:** e-Signed date

ORDER

Sub : Usage of Aadhaar – Dos & Don'ts for Sub-AUAs/Sub-KUAs - *Regarding*.

1. A Sub-AUA (Sub-Authentication User Agency)/Sub-KUA (Sub-KYC User Agency) is responsible for submitting the resident's Aadhaar number and demographic/biometric/OTP information, to the Central Identities Data Repository (CIDR), for the purpose of authentication.
2. A Sub-AUA/Sub-KUA is engaged in providing Aadhaar authentication Services to an Aadhaar number holder, as facilitated by the Authentication User Agency/ KYC User Agency (AUA/KUA). DoIT&C is registered as an AUA & KUA under UIDAI. The Sub-AUA/Sub-KUA are government departments / organizations / PSUs of Govt. of Rajasthan, which are authorized to use Aadhaar authentication services of UIDAI through DoIT&C and send authentication requests to enable its services / business functions.
3. Following are the Dos and Don'ts to be followed by the Sub-AUAs/Sub-KUAs:

DOs

(1) Sub AUA/ Sub KUA should ensure that it has a designated Chief Information Security Officer (CISO) and Deputy CISO that oversees information security governance and compliances. CISO should be appointed as per DoIT&C's letter no. F11(408)/DoIT/Project/2020-00714/BSDC-136 dated: 19-05-2025 (Copy enclosed). CISO should be in charge of the security of system, access control, audit, etc. and shall be responsible for protecting Aadhaar linked personal data.

(2) Read Aadhaar Act,2016 and its Regulations carefully and ensure all the compliance of provisions of the Aadhaar Act,2016 and its Regulations.

(3) Ensure compliance of the Information Security Policy for AUA/Sub-AUA/Sub-KUA issued by DoIT&C.(Link: https://aadhaar.rajasthan.gov.in/policyguideline.aspx?id=9CDF598)

(4) Ensure compliance of the Policy for Protecting Personal Data of Aadhaar Holders for AUA/KUA/Sub-AUA/Sub-KUA issued by DoIT&C.

(Link: https://aadhaar.rajasthan.gov.in/policyguideline.aspx?id=9CDF598)

(5) Ensure that everyone involved in Aadhaar related work is well conversant with provisions of Aadhaar Act, 2017 and its Regulations as well as processes, policies specifications, guidelines, circular etc. issued by UIDAI from time to time.

Signature valid
Digitally signed by Archana Singh
Designation : Commissioner and Secretary to Government
Date: 2025.08.25 11:17:06 IST
Reason: Approved

RajKaj Ref No.: 17330468

eSign 1.0

(6) Create internal awareness about consequences of breaches of data as per Aadhaar Act, 2016.

(7) Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

(8) Ensure regular training of operators/staff carrying out Aadhaar authentication on the best practices and safeguards involved in doing so.

(9) Follow the information security guidelines of UIDAI as released from time to time.

(10) Assure the resident about the security & confidentiality of their Aadhaar number being used for authentication.

(11) Informed consent - Aadhaar holder should clearly be made aware of the usage, the data being collected, and its usage. Aadhaar holder consent should be taken either on paper or electronically.

(12) Ensure that the resident clearly understand the type of data being collected and the purpose of Aadhaar authentication. Obtain resident's informed consent either on paper or electronically, prior to carrying out authentication.

(13) Store Aadhaar number only if you are authorized to do so and in the manner as prescribed by UIDAI i.e. within a secure Aadhaar Data Vault.

(14) Storage of Aadhaar no. and related eKYC data shall be only in a secure Aadhaar Data Vault and nowhere else. UIDAI's circulars dated: 18-07-2025 (copy enclosed) shall be followed in this regard.

(15) Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.

(16) For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number based index.

(17) Ensure that Aadhaar data collected is not shared with any entity except in accordance with the Aadhaar Act and/or regulations thereof.

(18) Verify that all data capture point and information dissemination points (website, report etc) should comply with UIDAI's security requirements.

(19) Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.

(20) Retain the logs of authentication transactions (including that of consents taken) only for the period as prescribed under Aadhaar (Authentication and Offline Verification) Regulations,

Signature valid
Digitally signed by Archana Singh
Designation : Commissioner and Secretary to Government
Date: 2025.08.25 11:17:06 IST
Reason: Approved

RajKaj Ref No.: 17330468

eSign 1.0

2021 i.e. in live database for 2 years and up-to 5 years in archive. Purging of such logs upon expiry of the period shall also be in accordance to the Aadhaar Act or regulations thereof.

(21) Identify and prevent any potential data breach or publication of personal data.

(22) Ensure swift action on any breach personal data as per Information Security Policy for AUA & Sub-AUA issued by DoIT&C.

(23) Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.

(24) Ensure proper hygiene of the authentication devices being used so that there are minimal authentication failures.

(25) Immediately report any suspicious activity around authentication to UIDAI namely, suspected impersonation by resident, likely compromise of authentication keys of Sub-AUA/Sub-KUA, likely fraud by authentication operator(s) etc.

(26) Cooperate with UIDAI and/or agencies deputed by UIDAI for the purpose of any security/process audit as required by the Aadhaar Act/Regulations or any other directions in this regard from UIDAI. Ensure timely closure of audit observations/non-compliances, if any.

(27) Provide effective grievance handling mechanism to the resident via multiple channels like website, call center, mobile app, SMS, physical center etc.

(28) Regular Information Security, Application Security and Source Code review audits must be conducted to ensure Aadhaar number and linked data is protected.

(29) Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure all Aadhaar holders are able to use it effectively.

(30) Multi-factor for high security – When doing high value transactions, multi-factor authentication must be considered.

(31) Create Exception handling mechanism on following lines-

a) It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.

b) If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.

Signature valid
Digitally signed by Archana Singh
Designation : Commissioner and Secretary to Government
Date: 2025.08.25 11:17:06 IST
Reason: Approved

RajKaj Ref No.: 17330468

eSign 1.0

c) If the schemes is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.

d) If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.

e) All authentication usage must follow with notifications/receipts of transactions.

f) Get all the applications using Aadhaar audited &certified for its data security by appropriate authority such as STQC/CERT-IN.

g) Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

(32) Fulfill all your statutory obligations under the Aadhaar Act, 2016 including Penalties for contraventions (Section 29 and Chapter VIA of Aadhaar Act).

DON'Ts

(1) Do not aid or abet any unlawful action of any resident/authentication operator/other entity that is in contravention of laws/regulations and prescribed processes & directions.

(2) Do not share your authentication keys/certificates with any other entity.

(3) Do not share unique license keys/code as provided by UIDAI with any other entity.

(4) Do not store photocopies of Aadhaar letters and/or other physical/electronic forms of Aadhaar, if used for collecting Aadhaar, without first masking/redacting the first 8 digits of the Aadhaar number displayed on those documents.

(5) Do not store/share/publish the biometric information collected from the Aadhaar number holder for authentication.

(6) Do not act in contravention of the Aadhaar Act, 2016 and regulations thereof.

(7) Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.

(8) Do not store any Aadhaar based data in any unprotected end point devices, such as PCs, laptops or smart phones or tablets or any other devices.

(9) Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other

Signature valid
Digitally signed by Archana Singh
Designation : Commissioner and Secretary to Government
Date: 2025.08.25 11:17:06 IST
Reason: Approved

certificate/document. Aadhaar number if required to be printed, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed.

(10) Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar act. The purpose of use of Aadhaar information needs to be disclosed to the resident.

(11) Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.

(12) Do not locate servers or other IT storage system/devices having Aadhaar data outside of a locked, fully secured and access-controlled room

(13) Do not permit any unauthorized people to access stored Aadhaar data.

All Sub-AUAs/Sub-KUAs registered under AUA/KUA- DoIT&C shall adhere to the aforementioned points.

(Archana Singh)
Secretary & Commissioner

Ref. No: F11(76)/DoIT&C/2022/Vol-3-00145 **Dated:** e-Signed date

Copy to following for information and necessary action please:

1. S. P.S. to All ACS/Secretaries/Commissioners/Head of Departments, Govt. of Rajasthan.
2. Sr. P. S. to Secretary & Commissioner, DoIT&C, Jaipur.
3. All Group Heads/Project OICs, DoIT&C HQ/RISL, Jaipur.
4. OIC-Website, DoIT&C/RISL is requested to kindly publish this on DoIT&C & RISL website.
5. Guard File.

Signature valid
Digitally signed by Archana Singh
Designation : Commissioner and Secretary to Government
Date: 2025.08.25 11:17:06 IST
Reason: Approved

GOVERNMENT OF RAJASTHAN
Department of Information Technology & Communication

Ref.No.F11(408)/DoIT/Project/2020-00714/BSDC-136 Date: 19/5/2025

Subject: Appointment of Chief Information Security Officer (CISO) in all department / PSU/etc.
Reference: MeitY letter No. 6(12)/2017-PDP-CERT-IN dated 14/3/2017.

With reference to the subject mentioned above and in accordance with the directive issued by Ministry of Electronics and Information Technology (MeitY), all departments and their associated organizations are required to establish a structured mechanism for information security through the appointment of a Chief Information Security Officer (CISO).

In compliance with this directive, a letter (Ref. No. F11(408)/DoIT/Project/2020-00714/BSDC-101 dated 03.09.2024) was issued to all departments, requesting the nomination of a CISO. However, many departments have yet to provide the details of their appointed CISO, and some have not made the appointment in line with the prescribed guidelines as mentioned below:

- **Chief Information Security Officer (CISO):**
  A senior officer of Joint Secretary rank or equivalent from department should be designated as the CISO. The CISO should report directly to the Secretary/Principal Secretary of the respective department and will be responsible for the overall information security framework within the department.

- **Deputy Chief Information Security Officer (Deputy CISO):**
  The senior-most officer from the Department of Information Technology & Communication (DoIT&C) or the National Informatics Centre (NIC) within your department or its associated organizations should be appointed as the Deputy CISO. This officer will be responsible for implementing the Cyber Security Program and ensuring adherence to the Information Security Policy.

The progress on the appointment of CISOs across the state is being reported monthly to the Ministry of Home Affairs, Government of India, through the Home Department.

In view of the above directive and the increasing number of cybersecurity incidents, you are requested to nominate a CISO and Deputy CISO for the respective department, its associated organizations, and the details may be sent to DoIT&C at RSOC@rajasthan.gov.in.

It is requested that the appointment process be completed by June 30, 2025.

Encl: Roles &Responsibilities of CISO

(Archana Singh)
Secretary, IT&C

All Addl. Chief Secretary/
Principal Secretary/ Secretary

Ref.No.F11(408)/DoIT/Project/2020-00714/BSDC-136 Date: 19/5/2025

Copy to following for Information & necessary Action:

- Joint Secretary, Chief Secretary Office, Govt. of Rajasthan
- PS to Secretary, DoIT&C

Signature valid
Digitally signed by Archana Singh
Designation: Commissioner and Secretary to Government
Date: 2025.05.17 17:27:18 IST
Reason: Approved

Joint Secretary

F. no.: HQ-13031/1/2022-AUTH-I HQ (Comp No. 13927)
Unique Identification Authority of India
(Authentication and Verification Division)

UIDAI Head Office, Bangla Sahib Road,
Gole Market, New Delhi – 110001
Dated: 18 .07.2025

Circular No. 8 of 2025

Subject: Revised guidelines for hosting Aadhaar Data Vault (ADV), Hardware Security Module (HSM) and authentication application on premises and cloud infrastructure for Aadhaar Authentication Ecosystem.

This circular shall be read in continuation of UIDAI circular no. 11020/205/2017-UIDAI (Auth-I) dated 25.07.2017 on ADV implementation and circular no. 11020/204/2017-UIDAI (Auth-I) dated 22.06.2017 on HSM implementation.

2. All requesting entities (REs) storing Aadhaar numbers, UID Tokens and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and demographic data) are directed to mandatorily implement the ADV.

3. Storage of Aadhaar number, UID Token or any Aadhaar demographic data received after successful Authentication or eKYC shall only be permitted within the ADV. Requesting entities are strictly prohibited for storing Aadhaar number or related data from the requested inputs by the Aadhaar number holder in Authentication/eKYC request.

4. The ADV implemented by a requesting entity must be hosted on either of the following:
   (a) on-premises (within the secure premises of the requesting entity);
   (b) on a Government Community Cloud (GCC) platform-based cloud, empaneled by MeitY (Ministry of Electronics and IT), Govt. of India; and
   (c) ADV as-a-service provided by an entity.

5. In case of GCC platform-based cloud implementation or ADV as-a-service based implementation, annual System and Organization Controls (SOC 2) Type II audit of the cloud infrastructure must be ensured by the concerned requesting entity.

6. Requesting entities must ensure the following for ADV implementation:
   (a) The GCC provider or the entity providing ADV as-a-service must be compliant with UIDAI security and privacy standards and ensure complete logical segregation of ADV for each requesting entity.
   (b) The data in ADV shall be stored in a single logical instance for each entity with the corresponding reference key which must be generated and used.
   (c) Aadhaar data must be stored in an encrypted format using strong algorithms like AES-256 or above.
   (d) High Availability and Disaster Recovery (HA/DR) shall be in place for the ADV with the same level of security along with dual redundant connectivity to the ASAs. It should have sufficient bandwidth based on respective anticipated transaction volume.
   (e) Only trusted communication channels, and secure APIs/microservices, shall be used for data access in vault.

(f) All access must be routed through authenticated applications with appropriate user authentication, authorization and logging mechanisms.

(g) Robust access control, monitoring and alerting systems must be implemented to detect and prevent unauthorized access to ADV. Ensure strict implementation of Identity and Access Management (IAM) so that only authorized personnel and systems can access the vault. All access must be logged and monitored.

7. Requesting entities and Authentication Service Agencies (ASA) must mandatorily implement the Hardware Security Module (HSM) for cryptographic operations (such as signing of authentication request, encryption/decryption of ADV data, decryption of eKYC response data or any other operation as mandated by UIDAI time to time). The HSM must be hosted as either of the following:

(a) on-premises (within the secure premises of the requesting entity),

(b) on a Government Community Cloud (GCC) platform-based cloud, empanelled by MeitY (Ministry of Electronics and IT), Govt. of India,

(c) as HSM services provided along with ADV as-a-service by any entity.

8. Requesting entities and ASAs must ensure the following for HSM implementation:

(a) It must be FIPS 140-2 Level 3 certified or higher,

(b) It must be logically isolated for each requesting entity/ASA independently.

(c) It must support:

(i) Key Generation

(ii) Secure Key Storage

(iii) Multifactor, Multirole Access Control and Audit Logging

9. The application should rotate the key, and the requesting entity/ASA must have a mechanism in place for the prevention of unauthorized substitution of keys.

10. Aadhaar authentication applications or any module handling authentication data shall only be hosted on-premises (within the secure premises of the requesting entity) *or* on a MeitY-empanelled platform.

11. Requesting Entities and ASAs are advised to refer the latest list of MeitY-empanelled GCC services provider, available at: *https://www.ambud.meity.gov.in*. This list is maintained and updated by MeitY.

12. This issues with the approval of competent authority.

(Pratik Choudhary)
Deputy Director
Tel.: 011-23478608
Email: dd1.auth-hq@uidai.net.in

To:

1. All requesting entities and Authentication Service Agencies in Aadhaar Authentication Ecosystem

Copy to:

1. Technology Centre, UIDAI, Bangalore
2. Regional Offices, UIDAI