

सं . के- के-11022/463/2016-यूआईडीएआई (ऑथ-1)

भारत सरकार  
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय  
भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)  
ऑथेंटिकेशन डिवीज़न

यूआईडीएआई मुख्यालय भवन, तीसरी मंजिल,  
बंगला साहेब रोड, काली मंदिर के पीछे,  
गोल मार्केट, नई दिल्ली- 110001  
दिनांक: 15.11.2022

To,

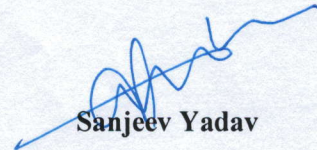
All AUAs / KUAs

**Sub:** Roll out of RE Compliance Checklist V3.0 for Annual IS Audit

Please refer Regulation 14(1)(h) of Aadhaar (Authentication and Offline Verification) Regulations 2021, wherein a requesting entity needs to "ensure that its operations and systems are audited by information systems auditor certified by a recognized body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request". Further, similar audit requirement is also laid down in Section 6(1) of the Aadhaar (Data Security) Regulations, 2016.

UIDAI is constantly engaged in upgrading and streamlining its procedures and systems, in accordance with the provisions of Aadhaar Act 2016 and associated regulations, to ensure security and confidentiality of identity information and authentication records of individuals.

In view of the above, the Competent Authority has approved "RE Compliance Checklist V3.0". All requesting entities are hereby directed to ensure compliance to this checklist and to make sure that Annual IS Audit for FY 2022-23 is done in accordance with new checklist from a CERT In empanelled auditor and adhere to provisions of Aadhaar Act 2016 and its Regulations, AUA/KUA Agreement, various guidelines and circulars issued by UIDAI.



Sanjeev Yadav  
(Director, Authentication)

**Enclosed:** RE Compliance Checklist V3.0



## Requesting Entity Compliance Checklist\_V3.0



### **Guidelines for the Auditor/Assessor:**

- 1.** Auditor must be CERT In empanelled for conducting IS Audit
- 2.** All below points need to be checked for the entire ecosystem of requesting entity including all applications, sub-contract agencies (where there are many sub-contractors reasonable sample agencies to be checked), SubAUAs (where there are many Sub-AUAs reasonable sample Sub-AUAs to be checked), physical and logical infrastructure of the requesting entity.
- 3.** The auditor/assessor is expected to mention details of the reason for compliance or non-compliance in the remarks section.
- 4.** The auditor/assessor is expected to provide reasonable evidences as part of the report to support the compliance status provided in the report.
- 5.** The auditor/assessor may add further points in this checklist to include details of the specifications/ requirements defined below. This is specifically for the points where the entire Regulation/ specification / notification / Circular / Policy etc. has been mentioned as a single checkpoint.



S.No.	Compliance Control	Yes/No/NA	Auditor Remarks
<b>1</b>	<b>Information to Aadhaar Number Holder</b>		
<b>1.1</b>	The requesting entity should obtain consent of an individual or in case of a child, the consent of the parent or guardian of the child before collecting their identity information for the purposes of authentication. The consent should be obtained in physical or preferably in electronic form.		
<b>1.2</b>	The requesting entity should ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication.		
<b>1.3</b>	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder or in case of a child, the consent of the parent or guardian of the child of the nature of information that will be shared by the Authority (UIDAI) upon authentication.		
<b>1.4</b>	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder or in case of a child, the consent of the parent or guardian of the child of the uses to which the information received during authentication may be put by it.		
<b>1.5</b>	At the time of authentication (before obtaining consent), requesting entity should inform the Aadhaar number holder or in case of a child, the consent of the parent or guardian of the child of the alternatives to submission of identity information.		
<b>1.6</b>	The requesting entity should also ensure that the information listed in 1.3, 1.4 and 1.5 is also communicated in local language.		
<b>1.7</b>	The requesting entity should maintain the logs for a. Record of consent of the Aadhaar number holder for authentication.		



	<p>b. Record of disclosure of information (as mentioned in point 1.3, 1.4, 1.5 and 1.6 above) to the Aadhaar number holder at the time of authentication.</p> <p>For any given Aadhaar number holder, whose identity information was collected, the requesting entity should be able to demonstrate that consent was taken and disclosure of information was made.</p>		
<b>1.8</b>	The consent taken from the resident should in accordance with the Aadhaar Act, 2016 and its regulations. No umbrella consent should be taken for sharing e-KYC or Aadhaar number of the residents with other entities.		
<b>1.9</b>	<p>If Applicable, the requesting entity should comply with the Notification No. 13012/79/2017/Legal-UIDAI (No. 6 of 2017) dated 19th December 2017 regarding "Process for placing and overriding bank accounts on Aadhaar Payment Bridge-National Payments Corporation of India (NPCI) Mapper". The requesting entity should comply with the following:</p> <p>a. Override request pertaining to an Aadhaar holder should be accompanied by the name of his current bank on the APB mapper and confirmation from the requesting bank that it has obtained the requisite consent of the Aadhaar holder for switching to the requesting bank on the mapper.</p> <p>b. Send request for mapping of a new account or overriding an existing bank account to NPCI only after taking explicit informed consent of their customers.</p> <p>c. Inform each account holder through sms and email within 24 hours that a request has been sent to NPCI to put his bank account on the mapper or, as the case may be, to change his bank account on the NPCI mapper (providing the name of current bank on the mapper and the last four digits of the account number of the new bank along with the bank name) and in case he does not want to put his</p>		



	<p>new bank account on the mapper, then the customer should be provided a methodology to reverse this mapping.</p> <p>d. If a customer does not have email or mobile number and communication cannot be sent, then his physical signature on a paper consent form should be obtained prior to sending the request to NPCI mapper.</p> <p>e. The records of consents obtained in (b) and the communications made in Para (a), (b), and (c) and scanned copy of the consent form in (d) shall be retained for 7 years by the banks as per the UIDAI Regulations.</p> <p>f. Make available the aforesaid records at the time of audit as per the provisions of Aadhaar (Authentication) Regulations, 2016.</p>		
<b>1.10</b>	The requesting entity should make provisions for sharing the consent related information with visually/audibly challenged divyangjan in an appropriate manner.		
<b>2</b>	<b>Security of the Authentication Devices and Applications</b>		
<b>2.1</b>	Requesting entity should capture the biometric information of the Aadhaar number holder using certified and registered biometric devices as per the standards specified by the Authority from time to time.		
<b>2.2</b>	Requesting entity shall necessarily encrypt and secure the biometric data at the time of capture as per the specifications laid down by the Authority.		
<b>2.3</b>	The client applications and software used for authentication should conform to standard APIs (latest) and specifications laid down by the Authority from time to time. Sub-AUAs should use client applications or (SDK) developed/digitally signed by AUA.		



<b>2.4</b>	After collecting necessary demographic and / or biometric information and/ or OTP from the Aadhaar number holder, the client application should immediately package and encrypt these input parameters into PID block before any transmission, and should send it to server of the requesting entity using secure protocols.		
<b>2.5</b>	AUA / KUA should ensure PID Block is encrypted with a dynamic session key using AES 256 symmetric algorithm (AES/GCM/NoPadding) at the time of capture on the authentication device. Session key, should be encrypted with 2048-bit UIDAI public key using asymmetric algorithm (RSA/ECB/PKCS1 Padding). The entity should comply with API Specification (Latest) document shared by authority time to time.		
<b>2.6</b>	The entity should ensure with respect to above, that Session key must not be stored anywhere except in memory and should not be reused across transactions. Only re-use of session key is allowed when its use as seed key when using synchronized session key scheme.		
<b>2.7</b>	<p>In the case of assisted devices and applications where operators need to mandatorily perform application functions, operators should be authenticated using multi factor authentication scheme like user id, password, Aadhaar Authentication, Answer to personal security questions, soft token, hard token, one time password, voice recognition, biometric data match, Pin etc.</p> <p>Under no circumstances should the assisted devices and "any application associated for Aadhaar Authentication" store the Aadhaar number, biometrics and/or e-KYC of the resident. It's essential for entities to maintain audit records for all the authentication request along with the response in compliance with regulations published by the authority.</p>		



<b>2.8</b>	Requesting Entity should implement strong governance and technical security control/ solution (Few example for internet access control are Training and awareness, Developing Acceptable use policy, URL/DNS filtering, Firewall, Network access control's, Proxy Server etc. ) to restrict, govern and monitor internet access for operator as well as staff to ensure they only have access to white listed or management approved website's over internet using devices leveraged to access or handle Aadhaar authentication device or application or data.		
<b>2.9</b>	The requesting entity should comply with all the requirements of UIDAI Circular K11022/460/2016-UIDAI (Auth-II) dated 28 February 2017. (Instruction for providing Authentication or eKYC Services by AUA KUA to Sub-AUA.		
<b>2.10</b>	Requesting entity should ensure Finger Minutiae Record (FMR) and Finger Image Record (FIR) should capture in single PID block for finger print based biometric authentication devices. The requesting entity should comply with UIDAI circular K 11022/198/2017-UIDAI (Auth-I) dated 11 November 2021.		
<b>2.11</b>	All the biometric devices used for Aadhaar authentication shall be registered with the server of the requesting entity.		
<b>2.12</b>	AUA / KUA monitor the operations of its devices and equipment, on a periodic basis, for compliance with the terms and conditions, standards, directions, and specifications, issued and communicated by the Authority, in this regard, from time to time.		
<b>2.13</b>	Entity should ensure operator employed for performing authentication function's and for maintaining necessary system and infrastructure, and process'(s) requisite qualification for undertaking such works.		



<b>2.14</b>	Entity should maintain details of devices and operators in assisted mode by maintaining proper logs of the operator with name of operator, deviceID, date and time etc. These logs should be verified by entity at regular periods. Entity should ensure they comply to Advisory regarding strengthening of Biometric authentication security, File number 13043/2/2021- AUTH-1-HQ dated 31 May 2022.		
<b>2.15</b>	Entity should ensure information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected against access, use and disclosure not permitted under Aadhaar (Authentication and offline verification) regulation, 2021.		
<b>3</b>	<b>Network, systems, key management and Data vault requirements</b>		
<b>3.1</b>	Requesting entity should establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication.		
<b>3.2</b>	Requesting entity should establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests.		
<b>3.3</b>	Requesting entity should ensure secure leased line connectivity with the CIDR compliant with UIDAI's standards and specifications, and also offer their UIDAI-compliant network connectivity as a service to Authentication User Agencies (AUAs)/ KYC User Agencies (KUAs) and transmit AUAs'/KUAs' authentication requests to CIDR. Only agencies contracted with UIDAI as ASAs shall send authentication requests to CIDR and no other entity can directly communicate with CIDR.		
<b>3.4</b>	Entity should perform source code review of the modules and applications used for Authentication and e-KYC and undergo audit by a certified auditor		



	and audit plan include organization information security policy inclusive of vulnerability assessment as well as penetration test on entity network, infrastructure and application.		
<b>3.5</b>	Requesting entity should employ only devices, equipment, or software, which are duly registered with or approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose.		
<b>3.6</b>	<p>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 latest standard compliant.</p> <p>Requesting entity should comply with all the requirements of UIDAI circular K 11020/204/2017-UIDAI (Auth-I) dated 22 June 2017 (Implementation of HSM by Entity/ASA).</p>		
<b>3.7</b>	<p>Requesting entity (which is allowed to store Aadhaar number) and other entities are mandatorily required to collect and store Aadhaar number and any connected data on a separate secure database/vault/system termed as "Aadhaar Data Vault". This will be the only place where Aadhaar number and any connected data should be stored.</p> <p>Each Aadhaar number is to be referred by an additional key called as Reference key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault. The requesting entity should comply with all the requirements of the UIDAI circular K-11020/205/2017-UIDAI (Auth-I) dated 25 July 2017 (Circular for Aadhaar Data Vault)</p>		
<b>3.8</b>	Entity should ensure all the end device used and asset's used should be used only after hardening to		



	reduce/eliminate the attack vector and condense the system attack surface.		
<b>3.9</b>	Requesting entity should ensure there are necessary data security measure implemented which such as data leakage prevention solution or alternative measure, Network intrusion and prevention systems/solution, Patch Management, encryption and identification and authentication mechanism, example DMZ, IPS/ IDS, WAF/Firewall, IAM solution etc. Entity should ensure to comply with Regulation 5, of Aadhaar (Data Security) Regulations, 2016.		
<b>3.10</b>	USB access on the servers and endpoints shall be restricted for all and should only be allowed on approval basis.		
<b>3.11</b>	Internet access on the systems shall be limited to the necessary or work related websites. Web portals known for pirated softwares, gambling etc. shall be restricted for accessing.		
<b>3.12</b>	Privileged accounts such as NTAuthority, Administrator and root accounts shall be accessible to limited set of users. Access to privileged account shall not be allowed to normal users.		
<b>4</b>	<b>Security Framework Policies for Requesting Entities</b>		
<b>4.1</b>	For better decoupling and independent evolution of various systems, it is necessary that Aadhaar number/ Virtual ID be never used as a domain specific identifier. In addition, domain specific identifiers need to be revoked and/or re issued and hence usage of Aadhaar number as the identifier does not work since Aadhaar number is permanent lifetime number. Example: Instead of using Aadhaar number as bank customer id or license number or student id, etc., always have a local, domain specific identifier and have the mapping in the backend database.		
<b>4.2</b>	Entity should ensure that the Aadhaar number/Virtual ID/ANCS Token provided by the		



	resident for authentication request shall not be retained by the device operator or within the device or at the AUA server(s).		
<b>4.3</b>	A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely: a. specified parameters of authentication request submitted; b. specified parameters received as authentication response; c. the record of disclosure of information to the Aadhaar number holder at the time of authentication; and d. record of consent of the Aadhaar number holder for authentication, but shall not, in any event, retain the PID information, Aadhaar Number/Virtual ID		
<b>4.4</b>	The logs of authentication transactions should be stored for audit purposes for 2 years online and then archived for 5 years.		
<b>4.5</b>	Entity should use licensed malware and antivirus solution (preferable next generation) to protect against malware's. The malware/Anti-Virus installed should be configured to update in real time.		
<b>4.6</b>	Annual standard certification and audit process should be established for applications, devices, and overall networks across the ecosystem and also to ensure the compliance to standard security policy and procedure.		
<b>4.7</b>	Wherever possible, only the domain specific identifier should be captured at the device end and not the Aadhaar number/ Virtual ID. For e.g. — Wherever possible, requesting entities should only capture their domain specific identifier (bank a/c no, ration card no along with family member id, LPG customer account no, etc.)		



	– On the requesting entity server, when forming the authentication input XML, retrieve the Aadhaar number from requesting entity database using domain specific identifier.		
4.8	Requesting entity should ensure the license keys are kept secure and access controlled. Separate license keys must be generated by AUA for their Sub-AUAs from the UIDAI portal.		
4.9	Requesting entity should establish a Data privacy policy addressing the privacy aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications. Such policy shall also be compliant to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. Such policy shall be published on the website of requesting Entity.		
4.10	The requesting entity shall ensure that it has provisions for annual reviews and assessments of its systems, infrastructure, etc., by a CERT-In empanelled agency to ensure compliance with Aadhaar Act, Regulations and specifications.		
4.11	Requesting entity should establish an Information Security Policy and Procedures addressing the security aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications.		
<b>5</b>	<b>Compliance Requirements</b>		
5.1	The requesting entity has to set up an effective grievance handling mechanism and provide the same via multiple channels.		
5.2	The requesting entity should be in compliance with the Intellectual Property provisions as defined in the agreement with UIDAI.		
5.3	The requesting entity shall mask Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters by redacting the first 8 digits of the Aadhaar number before storing the physical copies.		



<b>5.4</b>	The requesting entity should comply with the Aadhaar Act, 2016.		
<b>5.5</b>	The requesting entity should comply with Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
<b>5.6</b>	The requesting entity should comply with Aadhaar (Data Security) Regulations, 2016.		
<b>5.7</b>	The requesting entity should comply with Aadhaar (Sharing of Information) Regulations, 2016.		
<b>5.8</b>	The requesting entity should comply with UIDAI Information Security policy in respect to Entity available in the compendium on UIDAI official website.		
<b>5.9</b>	The requesting entity should comply with Aadhaar Do's and Don'ts available in the compendium on UIDAI official website.		
<b>5.10</b>	The requesting entity 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)		
<b>5.11</b>	The requesting entity should comply with provisions of AUA / KUA Agreement with UIDAI at all times.		
<b>5.12</b>	The requesting entity should comply with all the requirements of UIDAI circular K11022/460/2016-UIDAI (Auth-II) dated 6 July 2017 (Appointment of Sub-AUA – Application & Undertaking).		
<b>5.13</b>	The requesting entity should comply with all the requirements of UIDAI circular K11022/631/2017-UIDAI (Auth-II) dated 27 November 2017 (Sharing of e-KYC data with their Sub-AUAs).		



<b>5.14</b>	The requesting entity 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).		
<b>5.15</b>	The requesting entity 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).		
<b>5.16</b>	The requesting entity 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).		
<b>5.17</b>	The requesting entity 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).		
<b>5.18</b>	The AUAs should comply with Regulation number 15, Chapter-III, Aadhaar (Authentication) Regulations, 2016 Further clarified by: 1. UIDAI Circular No. F.No.K11022/460/2016-UIDAI (Auth-II), dated 28 February 2017 2. UIDAI Circular No. F.No.K11022/460/2016-UIDAI (Auth-II), dated 06 July 2017.		
<b>5.19</b>	The KUAs should comply with Regulation number 16, Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
<b>5.20</b>	The Requesting Entity should comply with Regulation number 22, Chapter-III, Aadhaar (Authentication and Offline Verification) Regulations, 2021.		
<b>5.21</b>	The Requesting Entity 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.		
<b>5.22</b>	The Requesting Entity should comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016.		
<b>5.23</b>	<p>AUAs / KUAs shall ensure that its operations and systems are audited by an information systems auditor certified by a recognized body on an annual basis and on a need basis to ensure compliance with UIDAI standards and specifications. The audit report shall be shared with UIDAI upon request; If any non-compliance is found as a result of the audit, management shall:</p> <ul style="list-style-type: none"> <li>a) Determine the causes of the non-compliance;</li> <li>b) Evaluate the need for actions to avoid recurrence of the same;</li> <li>c) Determine and enforce the implementation of corrective and preventive action;</li> <li>d) Review the corrective action taken</li> </ul> <p>The entity should ensure to comply with Regulation Aadhaar (Data Security) Regulations, 2016.</p>		
<b>5.24</b>	Requesting entity should while sharing data between two department for the purpose of formulation of scheme and selection of beneficiaries, burrowing department should seek consent of the beneficiary. Entity should comply with Aadhaar (Sharing of Information) Regulation, 2016 and File number H.Q- 13079/55/2021- AUTH-II HQ (Comp. No. 6074)/Government of India, Ministry of Electronic and Information's Authority of India		
<b>5.25</b>	Requesting entity should share semi masked Aadhaar card holder data if the data sharing is between different entity like central government and state for any other scheme. Entity should comply with Aadhaar (Sharing of Information) Regulation, 2016 and File number H.Q- 13079/55/2021- AUTH-II HQ (Comp. No. 6074)/Government of India,		



	Ministry of Electronic and Information's Authority of India		
<b>5.26</b>	The Requesting Entity should comply with all the circulars, notices, mandates issued by UIDAI from time to time.		
<b>5.27</b>	AUA and ASA should ensure message security and integrity between there server's, and third party entity as Sub-AUA/Sub-KUA.Entity should procure digital certificate should be procured from a valid certification authority as per Indian IT Act (see <a href="http://www.cca.gov.in/cca/?q=licensed_ca.html">http://www.cca.gov.in/cca/?q=licensed_ca.html</a> )		
<b>5.28</b>	Entity should ensure private key used for digitally signing the authentication request and the license keys are kept secure and access controlled. The private key should meet below parameter specified by the authority and documented in SPI Specification document (latest):-  a) Digital signature certificate used/ procured should be of class II or class III certificate		
<b>5.29</b>	Entity should connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronization of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC. Reference- CERT-In Directive No. 20(3)/2022-CERT-In dated April 28, 2022.		
<b>5.30</b>	Entity should ensure Authority to be informed of the ASAs with whom it has entered into agreements, and obtain approval from the Authority before appointing any third party entity as Sub-AUA/Sub-KUA. Entity should also ensure that third party entity as Sub-AUA/Sub-KUA operations and systems are audited by information systems auditor		



	certified by a recognized body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;		
<b>6</b>	<b>Compliance to UIDAI Information Security Policy for AUA/KUA as per compliance control 5.7</b>		
<b>6.1</b>	Entity shall appoint a Technical and Management SPOC for Aadhaar related activities and communication with UIDAI. Entity shall also inform UIDAI about the appointment of any new SPOC.		
<b>6.2</b>	Entity shall conduct a background check and sign a confidentiality agreement/NDA with all personnel/agency handling Aadhaar related information. Access to Authentication infrastructure shall not be granted before signing NDA and completion of BGV for personnel.		
<b>6.3</b>	AUA / KUA shall take an undertaking from BCs / similar entities (if applicable), Sub AUAs and other third party contractors regarding NDAs and BGVs conducted successfully for their personnel handling Aadhaar related data		
<b>6.4</b>	Information security trainings shall be conducted for all Entity personnel including BC/ similar entities for Aadhaar related authentication services during induction and subsequently on periodic basis. Specific and specialized training shall be conducted for various functional roles involved in authentication ecosystem. The training shall include all relevant security and data privacy guidelines as per the UIDAI information security policy for Authentication, Aadhaar Act, 2016, Aadhaar Regulations, 2016 and all circulars/notices published from time to time.		
<b>6.5</b>	Entity personnel including BC/ similar entities training shall be conducted half yearly and as and when changes are made in the authentication ecosystem. Entity shall maintain records of such trainings conducted.		



<b>6.6</b>	Entity 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.		
<b>6.7</b>	Before sending any equipment out for repair, the equipment shall be sanitized to ensure that it does not contain any Aadhaar related data. A movement log register of all the equipment sent outside shall be maintained.		
<b>6.8</b>	Entity should ensure only authorized individuals can access information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information. Entity should ensure the access is provided based on least privilege and access should be reviewed periodically.		
<b>6.9</b>	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.		
<b>6.10</b>	The AUA/KUA servers should be placed in a secure cabinet in the AUA Data Centre.		
<b>6.11</b>	<p>AUA/KUA Data Center hosting Aadhaar related information shall be fully secured and access controlled.</p> <p>AUA/KUA Data Center shall be manned by security guards during and after office hours CCTV surveillance shall cover the AUA/KUA servers.</p> <p>Access to the AUA/KUA Data Center shall be limited to authorized personnel only and appropriate logs for entry of personnel should be maintained.</p>		



	<p>Physical access to AUA Data Center and other restricted areas hosting critical Aadhaar related equipment/information shall be pre-approved and recorded along with the date, time and purpose of entry.</p> <p>The movement of all incoming and outgoing assets related to Aadhaar in the AUA/KUA Data Center shall be documented.</p> <p>Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall be posted at all entrances and at other points along the restricted areas.</p>		
<b>6.12</b>	Lockable cabinets or safes shall be provided in the AUA/KUA Data Center and information processing facilities having critical Aadhaar related information. Fire doors and fire extinguishing systems shall be deployed, labeled, monitored, and tested regularly.		
<b>6.13</b>	Preventive maintenance activities like audit of fire extinguishers, CCTV shall be conducted quarterly.		
<b>6.14</b>	<p>Personnel involved in operational/development/testing functions shall not be given additional responsibilities in system administration processes, audit log maintenance, security review of system or process and which may compromise data security requirements.</p> <p>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.</p>		
<b>6.15</b>	AUA / KUA personnel shall not intentionally write, generate, compile copy or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any		



	Aadhaar information.		
<b>6.16</b>	The Test and Production facilities / environments must be physically and/or logically separated.		
<b>6.17</b>	The AUA / KUA server shall reside in a segregated network segment that is isolated from the rest of the network of the AUA / KUA organization. The AUA / KUA server shall be dedicated for the online Aadhaar Authentication purposes and shall not be used for any other activities not related to Aadhaar.		
<b>6.18</b>	<p>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.</p> <p>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.</p>		
<b>6.19</b>	AUA / KUA must have its Aadhaar related servers hosted in data centers within India.		
<b>6.20</b>	Each authentication device shall have a Unique Device Code. A unique transaction number shall be generated automatically by the authentication device which should be incremented for each transaction processed.		
<b>6.21</b>	Entity 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.		
<b>6.22</b>	AUA / KUA shall ensure that the sub-AUAs, BCs and other sub-contractors are aware about Aadhaar		



	Authentication related incident reporting.		
<b>6.23</b>	Entity should document all changes to Aadhaar authentication applications, Infrastructure, processes and Information Processing facilities, and maintain Change log/ register.		
<b>6.24</b>	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.		
<b>6.25</b>	AUA/KUA shall not publish any personal identifiable data including Aadhaar in public domain/websites etc.		
<b>6.26</b>	<p>The Aadhaar number holder shall be notified by the requesting entity about any authentication, through email and/or mobile number about success or failure of authentication on each request. Such notification/acknowledgement shall include entity's name, date and time of authentication, auth response code (for online authentication), last 4 digits of Aadhaar number and purpose of authentication, as the case may be.</p> <p>In case of authentication failure the requesting entity should, in clear and precise language, inform the resident about the reasons of authentication failure such as Suspended/Cancelled Aadhaar or Biometric/Aadhaar Locking.</p>		
<b>6.27</b>	Entity 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 of securely.		
<b>6.28</b>	Entity should ensure incident management framework is implemented in accordance to Information security policy requirement/circular with inclusion of forensic investigation. Entity shall		



	perform Root Cause Analysis (RCA) for major incidents identified in its as well as sub-contractors' (if any) ecosystem. It is recommended that AUA / KUA shall deploy as part of its systems, a Fraud Analytics module that is capable of analyzing authentication related transactions to identify fraud.		
<b>6.29</b>	Entity should implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication delivery of services to the residents.		
<b>6.30</b>	Entity should ensure that the Aadhaar number/Virtual ID/ANCS Token provided by the resident for authentication request shall not be retained by the device operator or within the device or at the AUA server(s).		
<b>6.31</b>	End user device used for developing, process and handling Aadhaar data and application should timeout after session is idle for more then 30 minute to 15 minute based on criticality of application.		
<b>6.32</b>	Entity should ensure to integrate secure software development during application and software development lifecycle, to ensure security requirement is embedded throughout the development phase. Developer should be periodically provided training to ensure they are aware of SSDLC process. ( Security testing ( Dynamic and Static, architectural testing, code review. penetration test, User acceptance testing etc).		
<b>6.33</b>	Entity should utilize test data or non-production data for testing of application or software during testing phase.		
<b>6.34</b>	Entity should implement process and procedure to perform periodic information security risk assessment on its third party having access to Aadhaar application and resident data.		



--	--	--	--

**Note:** In case of any interpretation issues between this checklist and Aadhaar Act or Regulations, the requesting entity should rely on the Aadhaar Act, its Regulations and other specifications issued by UIDAI.

**Declaration by Audit Organization**

I hereby declare that the above requirements have been audited and meet the UIDAI standards & Specifications.

Auditor Name:

Auditor Signature:

Date:

Seal/Digital Sign/Company Seal: