14.eSign Service Policy

QCID Technologies Private Ltd. Plot No 1303, Ayyappa Society, Madhapur, Hyderabad, Telangana, INDIA-500081.

14. eSign Service Policy

13.1 Policy Approvals		
Approved by	**Approval Date**	**Approved Version**
Board	27-Jul-2020	1.0
Board	24-Jan-2025	1.1
Board	24-Dec-2025	1.2

13.2 Document Version Control		
Version Number	**Version Date**	**Changes**
1.0	25-Jul-2020	Final
1.1	24-Jan-2025	Added Annexure I to the directions dated 28.4.2022 of CERT-In, bearing no. 20(3)/2022-CERT-In Modified Reporting time 24 hours to 6 hours related to confidentiality breach/security/Cyber Incidents
1.2	23-Dec-2025	Added Control No 6.13
1.3	27-Apr-2026	Added Control No 6.14

13.2.1 Revision Control		
Revision No	**Revision Date**	**Revision Done by**
1.0	02-Mar-2021	Avinash
1.1	22-Feb-2022	Avinash
1.2	29-Mar-2023	Avinash
1.3	12-Jun-2024	Avinash
1.4	04-Jun-2025	Avinash
1.5	14-Jul-2026	Avinash

13.3 Document Ownership		
Document Owner	**:**	**Chief Executive Officer**

13.4 Purpose:
The purpose of this policy is to handle security of UIDAI information assets by QCID and their partners for providing services. The confidentiality, integrity and availability of these always be maintained by QCID and their partners.

13.5 Scope and Applicability:
This policy is applicable wherever Aadhaar related information is processed or stored by

14. eSign Service Policy

QCID Technologies and their Partners.

1. **Authentication User Agencies:** Authentication user Agency is a requesting entity that uses Yes/ No Authentication facility service provided by UIDAI;
2. **KYC User Agencies:** KYC User Agency is a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by UIDAI.

AUA connects to the central Identities Data Repositories (CIDR) through ASA.
AUA/ KUA user's demographic data, and/or biometric data in addition to resident's UID

13.6 Definitions:

Personal data – 'Personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier. (ex: Aadhar Number)

13.7 Acronyms:

AUA: Authentication User Agency

KUA: KYC User Agencies

ASA: Authentication Service Agency

CIDR: Central Identities Data Repositories

13.8 Policy

1. **Information Security Policy for AUAs and KUAs:** In addition to information security policy, the QCID will implement the controls applicable to Authentication User Agencies (AUAs) / KYC User Agencies (KUA) and partners who are handling the Aadhaar Authentication.

2. **Human Resources:** In addition to HR Security Policy, the QCID appointed a Technical and point of Contact Person (POC) for Aadhaar related activities and communication with UIDAI. QCID will also inform UIDAI about the appointment of any new POC.
   - 2.1 QCID conducted background check and signed a confidentiality agreement/NDA with all personal/ agency handling Aadhaar related information and for not handling Aadhaar related information personal.
   - 2.2 Information security and data privacy training will be conducted by QCID for all the Partners before onboarding, the training will be also conducted when changes occur and also once a year.
   - 2.3 Special training will be conducted for various functional roles involved in authentication.
   - 2.4 Access to authentication infrastructure will not be granted before signing NDA and completion of BGV for personnel.

3. **Asset Management:** In addition to Asset Management Policy, all assets used by QCID (business applications, operating systems, databases, network etc.) for the purpose of delivering services to residents using Aadhaar Authentication services will be identified, labelled and classified.
   - 3.1 Details of the information asset will be recorded, and an asset inventory will be maintained and updated as and when required as per Asset management policy.
   - 3.2 As per Data Retention and Disposal Procedure document, QCID will follow the procedure for disposal of the information assets being used for authentication operations. Information systems / documents containing Aadhaar related information for disposing of data securely.
   - 3.3 As per Data Retention and Disposal Procedure document, QCID will follow the procedure before sending any equipment out for repair, the equipment will be sanitized to ensure that it does not contain any Aadhaar related data. The equipment sent outside will be registered once it is approved by management.
   - 3.4 QCID will not transfer or make an unauthorized copy of any Aadhaar related information including identity information to any personal device or other unauthorized electric media / storage devices. The personal storage will be disabled to connect to QCID network.
   - 3.5 QCID implemented controls to prevent and detect any loss, damage, theft or compromise of the assets containing any Aadhaar related information.
   - 3.6 QCID will control and allow the authentication devices used to capture resident's biometric are STQC certified registered devices. QCID will allow all the sub-AUAs, Business correspondents or other sub-contractors to use the STQC certified registered devices only.
   - 3.7 As per the Asset Management Policy, the ownership of authentication assets will be clearly identified and documented.
   - 3.8 As per IT Security Operations Policy and Network Security Policy, all the assets will be hardened based on hardening standards unless specified by UIDAI.

4. **Access Control:** In addition to Access Control Policy, only authorized individuals will be provided access to information facilities (such as authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information. Access control list will be maintained by AUA/KUA.
   - 4.1 QCID and partners personnel with access to UIDAI information assets will behave least privilege access for information access and processing.
   - 4.2 Access rights and privilege to information processing facilities for Aadhaar related information will be revoked within 24 hours of exit of respective personnel. Past deactivation, user IDs will be deleted if not in use.
   - 4.3 Access rights and privileges to information facilities processing Aadhaar related information will be reviewed on a quarterly basis and the report will be maintained for audit purposes.
   - 4.4 Common user IDs / group user IDs will not be allowed. Exceptions shall be approved by QCID management and documented.
   - 4.5 Procedures are in place for secure storage and management of administrative passwords for critical information systems and access log register is maintained.
   - 4.6 Users are not provided with local admin access rights on their systems.

4.7 Successive login failures will result in user account being locked; they will not be able to login until account is unlocked and the password reset. The user needs to contact the system Administrators to get the account unlocked.

5. **Password Policy:** In addition to Authentication and password management, the allocation of initial passwords will be done in a secure manner, and these passwords will be changed at first login.
   5.1 All user passwords will remain confidential and will not be shared.
   5.2 Passwords being stored in the database or any other form, they will be stored in an encrypted /hashed form.
   5.3 Password will be changed whenever there is any indication of a possible system.
   5.4 As per Password Policy complex passwords will be used.
   5.5 Passwords are not hardcoded in codes, login scripts, any executable program or files.
   5.6 Passwords are not stored or transmitted in application in clear text.
   5.7 Passwords are not included in any automated log-on process.

6. **Cryptography and security of Aadhaar number:** In addition to IT Security Operations Policy, the Personal identity data (PID) block comprising of the resident's demographic/ biometric will be encrypted as per the latest API specifications rolled out by UIDAI.
   6.1 The PID will get encrypted at the end point device used for authentication and it will remain encrypted during transit and flow within the AUA / KUA and while sharing this information with ASAs.
   6.2 The encrypted PID block will 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.
   6.3 QCID while providing authentication services to Sub-AUAs other subcontracted entities will ensure that the client application used for Aadhar authentication is developed by QCID (AUA/KUA) and is digitally signed by the QCID (AUA/KUA).
   6.4 The keys used for digitally signing of authentication request and decryption of e-KYC XML Response will be stored in HSM only. The HSM used shall be FIPS 140-2 complaint.
   6.5 The QCID (AUA/ KUA) will follow all the HSM provisions as defined in the circular – 110202/ 204/2017 dated 22nd June 2017, and any subsequent guideline / circular notice published by UIDAI in this regard.
   6.6 The QCID (AUA/KUA) will follow all the HSM provisions as defined in the circular – 11020/204/2017 dated 22nd June 2017 and any subsequent guideline / circular / notice published by UIDAI in this regard.
   6.7 The authentication request will be digitally signed by the requesting entity and/ or by the Authentication Service Agency, as per the mutual agreement between them.
   6.8 As per Key Management Procedure, the Key management activities will be performed by all QCID (AUA / KUA) to protect the keys throughout their lifecycle.
   6.9 The reference key used for the Aadhaar Data Vault will be generated using Universally Unique Identifier (UUID) scheme so that Aadhaar Number will neither be guessed nor reverse engineered using the reference.

6.10 Full Aadhaar number display will 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 will be masked such that only the last four digits of the Aadhaar number are displayed.

6.11 Global and local AUA will make necessary changes in their authentication systems for use of Virtual token, UID token and Limited e-KYC.

6.12 AUA.KUA will integrate Virtual Token and UID Token into their services.

6.13 The QCID (AUA/ KUA) will not store Aadhaar numbers, The Aadhaar data will be stored in a UIDAI-compliant Aadhaar Data Vault (ADV) with tokenization, encryption, and strict access controls as per Circular 8 of 2025.

6.14 All Aadhaar authentication and e-KYC transactions shall use secure hashing algorithm of SHA-2 for digital signing as per Circular 4 of 2026.

7. **Physical and Environmental Security:** In addition to Phy and Env Security Policy, the AUA/KUA servers will be placed in a dedicated and isolated area in the Data Center.

7.1 AUA/KUA Data Center hosting Aadhaar related information will be fully secured, and access controlled.

7.2 AUA/KUA Data Center will be manned by security guards during and after office hours.

7.3 CCTV surveillance will cover the AUA/KUA servers.

7.4 Access to the AUA/KUA Date Center will be limited to authorized personnel only and appropriate logs for entry of personnel will be maintained.

7.5 The movement of all incoming and outgoing assets related to Aadhar in the AUA/KUA Data Center will be documented.

7.6 Lockable cabinets will be provided in the AUA/KUA Data Center and information processing facilities having critical Aadhar related information.

7.7 Fire doors and fire extinguishing systems will be deployed, labelled, monitored, and tested regularly.

7.8 Preventive maintenance activities like audit of fire extinguishers and CCTV will be conducted quarterly.

7.9 Physical access to AUA Data Center and other restricted areas hosting critical Aadhaar related equipment/ information will be pre-approved and recorded along with date, time and purpose of entry.

7.10 Signs or notices legibly setting forth the designation of restricted areas and provisions of entry will be posted at all entrances and at other points along the restricted areas as necessary especially where the AUA/KUA servers are physically hosted.

7.11 Controls will be designated and implemented to protect power and network cables from unauthorized interception or damage.

7.12 A clear desk and clear screen policy will be adopted to reduce risks of unauthorized access, loss and damage to information related to Aadhaar. Screen saver or related technological controls will be implemented beyond a specified duration.

7.13 Controls such as intrusion detection and evaluation plans will be implemented in case of an emergency.

8. **Operations Security:** In addition to Information Security Policy and IT Security Operations Policy, AUA/KUA will complete the Aadhaar AUA/ KUA on-boarding process as defined by UIDAI, before the commencement of formal operations.
   - 8.1 Information Security policy, processes, roles and responsibilities for Information security will be maintained by AUA/KUA for governance of information security.
   - 8.2 Standard Operating Procedure (SOP) will be developed for all information systems and services related to Aadhaar operations. The SOP will include the necessary activities to be carried out for the operations and maintenance of the system or service and to be taken in the event of a failure.
   - 8.3 AUA/KUA personnel will not intentionally write, generate, compile copy or attempt to introduce any computer code designated to damage or otherwise hinder the performance of, or access to, any Aadhar information.
   - 8.4 A formal patch Management Procedure will be followed.
   - 8.5 Periodic Vulnerability Assessment (VA) exercise will be conducted to ensure the security of the Aadhaar infrastructure.
   - 8.6 All hosts that connect to the Aadhaar Authentication Service or handle resident's identity information will be secured using endpoint security solutions. Anti-virus / malware detection software will be installed on such hosts.
   - 8.7 Network Intrusion and prevention systems will be in place - e.g. IPS, IDS, WAF, etc.
   - 8.8 AUA/KUA will ensure that the event logs recording the critical user-activities, exceptions and security events will be enabled and stored to assist in future investigations and access control monitoring.
   - 8.9 The AUA/KUA will follow all the consent related provisions as defined in the Aadhaar Act 2016, Aadhar Regulations 2016 and all circulars/notifications published from time to time.
   - 8.10 The AUA/KUA will maintain the logs of the Aadhaar authentication transaction as defined in the Aadhaar (Authentication) Regulations, 2016.
   - 8.11 The Aadhaar authentication logs will not, in any event, retain the PID information.
   - 8.12 The e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, will be shared with sub-AUA or any other entity after obtaining specific permission from UIDAI by applying in this regard. After obtaining the appropriate permissions, the said data may be shared as per provisions of the Aadhaar Act 2016, Aadhar Regulations 2016 and all provisions of the Aadhar Act 2016, Aadhaar Regulations 2016 and all circular/notifications published from time to time.
   - 8.13 The client application used for Aadhaar authentication by AUA/KUA, and its ecosystem partners will not store biometric data collected during authentication under any circumstances.
   - 8.14 The logs of authentication transactions will be maintained by the AUA/KUA as defined by Aadhar Act,2016, Aadhar Regulations 2016 and all circulars/notifications published from time to time.
   - 8.15 The AUA/KUA server will reside in a segregated network segment that is isolated from the rest of the network of the AUA/KUA organization. The AUA/ KUA server will be dedicated for the online Aadhaar authentication purposes and shall not be used for any other activities not related to Aadhaar.
   - 8.16 AUA/KUA, sub-AUAs, and other sub-contractors performing Aadhar authentication will 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.

8.17 No data pertaining to the resident, or the transaction will be stored within the terminal device.

8.18 Global AUAs and KUAs will store Aadhaar numbers and related information on a separate secure database/ vault/ system, which will be made secure and accessed through internal systems only. This Aadhaar Data vault must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.

8.19 Aadhaar number and any other data kept in the Aadhar data vault will keep in an encrypted format only.

8.20 The AUA/KUA will follow all the Aadhar Data vault provisions as defined in the circular – 11020/205/2017 dated 25th July 2017 and any subsequent guideline/circular/ notice published by UIDAI in the regard.

8.21 The AUA/KUA may be collecting biometric of residents for purposes other than those defined under the Aadhaar Act 2016, Aadhaar Regulations 2016 and all circulars/notifications published from time to time. In such cases, the Aadhaar number will not be linked with the biometric data collected for such other purposes.

8.22 KUA will not share its e-KYC license key with any other organization. Sub-AUAs or any other entity will not perform e-KYC using KUA's license key.

8.23 For better decoupling and independent evolution of various systems, it is necessary that Aadhaar number be never used as a domain specific identifier. In addition, domain specific identifiers need to be revoked and/or re-issued.

8.24 Separate license keys must be requested by AUA for their sub-AUAs, via UIDAI Auth-Support.

8.25 AUA/KUA will have its Aadhaar related servers hosted in data centers within India.

8.26 AUA/KUA will perform source code review of the modules and applications used for Authentication and e-KYC as well as vulnerability assessment and configuration assessment of the infrastructure.

9. Application Security:

9.1. AUA/KUA will ensure that all pages and resources of the modules and application used for authentication and e-KYC by default require authentication except those specifically intended to be public.

9.2. AUA/KUA will further ensure that there are no default passwords in use for the application framework or any components used by the application.

10. Communications Security:

10.1. Each authentication device will have a unique device code. This number will be transmitted with each transaction along with UIDAI assigned institution code for the AUA/KUA as specified by the latest UIDAI API documents.

10.2. A unique transaction number will be generated automatically by the authentication device which should be incremented for each transaction processed.

10.3. The network between AUA/KUA, its subcontractors and ASA will be secure. AUA/KUA will connect with ASAs through leased lines or private lines. If a public network is used, a secure channel such as SSL or VPN will be used.

10.4. The AUA/KUA server will be hosted behind a firewall. The firewall rules will block incoming access requests to the AUA/KUA server from all sources other than AUA/KUA's PoT terminals.

10.5. use of web-based e-mail shall be restricted to official use and in accordance with the acceptance usage guidelines or as per organizations policy.

11. Information Security Incident Management: In addition to Incident Management Policy, AUA/KUA will be responsible for reporting any security weaknesses, Incidents possible misuse or violation of any of the stipulated guidelines to UIDAI immediately.

11.1. AUA/KUA will ensure that the sub-AUAs, and partners are aware about Aadhaar Authentication related incident reporting.

11.2. AUA/KUA will perform Root Cause Analysis (RCA) for major Aadhaar related incidents identified in its as well as its sub ecosystem.

11.3. Any confidentiality breach/security breach of Aadhaar related information will be reported to UIDAI within 6 hours.

12. Compliance: In addition to Compliance Policy, the AUA/KUA will comply with the UIDAI AUA/KUA agreement, Aadhaar Act 2016, Aadhar Regulations 2016, as well other notices and circulars published by UIDAI from time to time.

12.1. The AUA/KUA will ensure that the application used for Aadhaar Authentication is audited by information system auditor(s) certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI. All Sub-AUAs shall also access authentication services only through duly audited client applications.

12.2. AUA will take permission from UIDAI before the appointment of an entity as their Sub-AUA. Also, shall take permission for already appointed Sub-AUAs.

12.3. AUA/KUA will ensure that its operations and systems are audited by an information systems auditor certified by a recognized body on an annual basis to ensure compliance with UIDAI standards and specifications and the same will be shared with UIDAI upon request.

12.4. In addition to the audits to be performed by AUA/KUA by itself on an annual basis, UIDAI may conduct audits of the operations and systems of AUA/KUA, either by itself or through an auditor appointed by UIDAI.

12.5. If any non-compliance is found because of the audit, management will:

a. Determine the causes of the non-compliance;
b. Evaluate the need for actions to avoid recurrence of the same;
c. Determine and enforce the implementation of corrective and preventive action; and
d. Review the corrective action taken.

12.6 AUA/KUA will use only licensed software for related infrastructure environment. Records of all software licenses will be kept and updated regularly.

12.7 AUA/KUA and their ecosystem of partners will ensure compliance to all the relevant laws, regulations as well as other notices, circulars and guidelines as defined by UIDAI from time to time.

12.8 it is recommended that AUA/KUA, deploy as part of its systems, a fraud analytics module that is capable of analyzing authentication related transactions to identifying fraud.

12.9 AUA/KUA will audit its sub-AUAs, or partners providing Aadhaar Authentication services as per all the relevant laws, regulations as well as other notices, circular and guidelines as defined by UIDAI from time to time.

12.10 for all authentication application deployed by an AUA/KUA and its Sub-AUA, the logo of an AUA/KUA will be clearly visible.

13. Data protection:

13.1. The AUA/KUA will inform the residents of the following details by providing a notice at the item of authentication.

a. The nature of information that will be shared by UIDAI upon authentication;

b. The uses to which the information received during authentication may be put; and

c. Alternatives to sub domain of identity information.

13.2 AUA/KUA will establish a data privacy policy addressing the privacy aspects of Aadhar as defined under Aadhar Act, Regulations and specifications, such policy will also be compliant to the Information Technology rules, 2011. Such a policy will be published on the website of AUA/KUA.

13.3 AUA/KUA will obtain the consent of the resident for authentication in physical or preferably in electronic form and maintain logs or records of the consent obtained.

13.4 AUA/KUA will maintain logs of authentication transactions for a period of years during which period an Aadhaar number holder will have the right to access such logs. Upon expiry of the 2 years period, the logs will be archived for a period of 5 years, or the number of years as required by laws or regulations governing the entity, whichever is later, and upon expiry of the said period, the logs will be deleted except Those records require to the retained by a court or required for any pending disputes.

13.5 The Aadhaar number holder may, at any time, revoke consent given to a KUA for storing his e-KYC data, received upon e-KYC authentication in encrypted form, or for sharing it with External partner, and upon such revocation, the KUA will delete the e-KYC data and cease any further processing.

13.6 AUA/KUA will:

a. Report promptly to UIDAI (within 6 hours) any privacy incidents affecting the personal data of the residents; and

b. Report promptly to 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. Extended full cooperation to UIDAI, or any agency appointed or authorized by UIDAI to cooperate while inquiries, incidents, claims and complaints are being handled in case of any security and privacy breach.

13.7 AUA/KUA upon termination of its services will ensure the following:

a. The arrangements for militance and preservation of authentication logs and other documents in accordance with procedures as may be specified by UIDAI for this purpose;
b. The arrangements for making authentication record available to the respective on such request;
c. Records of redressal of grievances, if any; and
d. Settlement of accounts with UIDAI, if any.

Further, the obligations relating to authentication logs will continue to remain in force despite termination of appointment.

14. **Change Management:** In addition to the Change Management procedure, AUA/KUA will document all changes to Aadhar authentication applications, infrastructure, processes, and information processing facilities.
Change log/ register will be maintained for all such changes performed.

13.9 Connected Reference Documents:		
Name	**Version Number**	**Description**
Information Security & Organization Policy	V 1.2	NA
Asset Management Policy	V 1.2	NA
HR Security Policy	V 1.2	NA
Phy and Env Security Policy	V 1.2	NA
IT Security Operations Policy	V 1.2	NA
Network Security Policy	V 1.2	NA
Info Exchange Policy	V 1.2	NA
Info Exchange Policy	V 1.2	NA
Access Control Policy	V 1.2	NA
App Sys Acq Dev and Maint Policy	V 1.2	NA
Incident Management Policy	V 1.2	NA
BCM Policy	V 1.2	NA
Compliance Policy	V 1.2	NA
Privacy Policy	V 1.2	NA
Change Management Procedure	V 1.2	NA
Key Management Procedure	V 1.2	NA
Third Party Information Security Policy	V 1.0	NA

13.10 Standards Covered:	
Name	**Controls / Sections**
Aadhaar Act 2016, 2019, 2022, 2025	ALL

QCID Technologies Private Ltd. Plot No 1303, Ayyappa Society, Madhapur, Hyderabad, Telangana, INDIA-500081.