SMART PAYMENT SOLUTIONS PRIVATE LIMITED

Model Authentication Compliance Policy for Requesting Entities

Version 1.0

Version control

Date	Version no.	Name of the author	Reviewer
01.02.2023	*1.0*	*Mr. Praveen Dhabhai*	*Mr.Prashant Kumar, IT Head*
	Approved by the Director, Mr. Naresh chandra Mangal		

Abbreviations

Abbreviation	Description
ADV	Aadhaar Data Vault
API	Application Program Interface
ASA	Authentication Service Agency
AUA	Authentication User Agency
BC	Business Correspondent
BGV	Background Verification
CCTV	Closed-circuit television
CERT-In	Indian Computer Emergency Response Team
CIDR	Central Identities Data Repository
e-KYC	Electronic Know Your Customer
e-Mail	Electronic Mail
HSM	Hardware Security Module
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
KUA	e-KYC User Agency
NDA	Non-Disclosure Agreement
NTP	Network Time Protocol
OTP	One-Time Password
PID	Personal Identity Data
POS	Point of Sale
PoT	Point of Transaction
RCA	Root Cause Analysis
SMS	Short Message Service
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSL	Secure Sockets Layer
STQC	Standardisation, Testing and Quality Certification
UIDAI	Unique Identification Authority of India
UID Token	Unique ID Token
UUID	Universally Unique Identifier

Abbreviation	Description
VA	Vulnerability Assessment
VID	Virtual ID
VPN	Virtual Private Network
WAF	Web Application Firewall
XML	Extensible Markup Language

Table of Contents

1. Terms and Definitions

a) ***"Aadhaar number"*** means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section.
Reference: Section 2(a) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and Section 3(i)(a) of the Aadhaar and Other Laws (Amendment) Act, 2019

b) ***"Aadhaar Data Vault" (ADV)*** means a separate secure database/vault/system where the entities mandatorily store Aadhaar numbers and any connected data such that it will be the only place where the said data will be stored.

Reference: Point number (a) Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25.07.2017

c) "***Authentication***" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.
Reference: Section 2(c) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

d) ***"Authentication Service Agency" or "ASA"*** shall mean an entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority.

Reference: Regulation number 2(f) of the Aadhaar (Authentication) Regulations, 2016

e) ***"Authentication User Agency"*** *or* ***"AUA"*** means a requesting entity that uses the Yes/ No authentication facility provided by the Authority.

Reference: Regulation number 2(g) of the Aadhaar (Authentication) Regulations, 2016

f) "***Authority***" means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

Reference: Section 2(e) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

g) "***Consent***" means the consent referred to in section 11 of PDP bill 2019

Reference: section 11 of PDP bill 2019 (given below)

11. (*1*) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

(2) The consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

(3) In addition to the provisions contained in sub-section (*2*), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—

(a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;

(b) in clear terms without recourse to inference from conduct in a context; and

(c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.

(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.

(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

h) "***Demographic information***" includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history.

Reference: Section 2(k) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

i) "***e-KYC User Agency***" or "***KUA***" shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority. Requesting Entity herein Smart Payment Solutions Private Limited(herein after referred as "SPSPL")

Reference: Regulation number 2(l) of the Aadhaar (Authentication) Regulations, 2016

j) "***Global AUAs***" means the agencies which will have access to full e-KYC (with Aadhaar number) and the ability to store Aadhaar number within their system.

Reference: Point number 9(a) of Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

k) ***"Local AUAs"*** means the agencies which will only have access to Limited KYC and will not be allowed to store Aadhaar number within their systems.

Reference: Point number 9(b) of Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

l) ***"Hardware Security Module (HSM)"*** *means a device that will store the keys used for digital signing of Auth XML and decryption of e-KYC response data received from UIDAI.*

Reference: Point number 4 of Circular No. 11020/204/2017 – UIDAI (Auth-I), dated 22.06.2017

m) "***Identity information***" in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information.

Reference: Section 2(n) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

n) "***Limited KYC***" means the service that does not return Aadhaar number and only provides an agency specific unique UID Token along with other demographic fields that are shared with the Local AUAs depending upon its need.

Reference: Point number 3 (II) and 9(b) of – Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

o) "***PID Block***" means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication.

Reference: Regulation number 2(n) of the Aadhaar (Authentication) Regulations, 2016

p) ***"Personnel"*** means all the employees, staff and other individuals employed/contracted by the requesting entities.

Reference: Regulation number 2 (1) (f) of Aadhaar (Data Security) Regulations 2016

q) **"*Reference Key*"** means an additional key which is mapped with each Aadhaar number stored in the Aadhaar data vault.

Reference: Point number (c) Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25.07.2017

r) **"*Requesting Entity*"** means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication.

Reference: Section 2(u) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

s) **"*Resident*"** means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment.

Reference: Section 2(v) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

t) ***"Sensitive personal data or information"*** means such personal information which consists of information relating to —

i. password;
ii. financial information such as Bank account or credit card or debit card or other payment instrument details;
iii. physical, physiological and mental health condition;
iv. sexual orientation;
v. medical records and history;
vi. Biometric information;
vii. any detail relating to the above clauses as provided to body corporate for providing service; and
viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise;

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Reference: Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

u) **"*UID Token*"** means a 72-character alphanumeric string returned by UIDAI in response to the authentication and Limited KYC request. It will be unique for each Aadhaar number for a particular entity (AUA/Sub-AUA) and will remain same for an Aadhaar number for all authentication requests by that particular entity.

Reference: Point number 10 of in Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

v) **"*Virtual ID (VID)*"** means any alternative virtual identity issued as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.

Reference: Section 3 (4) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and Section 4 of the Aadhaar and Other Laws (Amendment) Act, 2019

2. Purpose

The purpose of this policy is to provide direction to the various stakeholders and responsible personnel within **SPSPL** for deploying relevant security controls to secure the data of the Aadhaar number holder in compliance to the relevant provisions of the Aadhaar Act, 2016; the Aadhaar and Other Laws (Amendment) Act, 2019; the Aadhaar (Authentication) Regulations, 2016; the Aadhaar (Data Security) Regulations; the Aadhaar (Sharing of Information) Regulations, 2016.

3. Human Resources

a) A Technical and Management SPOC shall be appointed for Aadhaar related activities and communication with UIDAI. UIDAI shall also be informed about the appointment of any new SPOC.

b) **SPSPL** shall conduct a background check and sign a confidentiality agreement/NDA with all personnel/agency handling Aadhaar related information. UIDAI or agency appointed by UIDAI may validate this information.

c) **SPSPL** 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.

d) Information security trainings shall be conducted for all the personnel for Aadhaar related authentication services during induction and subsequently on periodic basis. The training shall include all relevant security 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.

e) Specific and specialised training shall be conducted for various functional roles involved in authentication ecosystem.

f) Training shall be conducted half yearly and as and when changes are made in the authentication ecosystem. Records of such training conducted shall be maintained.

g) Access to authentication infrastructure shall not be granted before signing NDA and completion of BGV for the personnel.

h) The user ID credentials and access rights of personnel handling Aadhaar related authentication data shall be revoked/ deactivated within 24 hours of exit of the personnel.

4. Asset Management

a) All assets used by **SPSPL** (business applications, operating systems, databases, network etc.) for the purpose of delivering services to residents using Aadhaar authentication services shall be identified, labelled and classified.

b) Details of the information asset shall be recorded, and an asset inventory should be maintained and updated as and when required.

c) **SPSPL** 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.

d) Before sending any equipment out for repair, the equipment shall be sanitised to ensure that it does not contain any Aadhaar related data. A movement log register of all the equipment sent outside shall be maintained.

e) **SPSPL** shall not transfer or make an unauthorized copy of any Aadhaar related information including identity information to any personal device or other unauthorized electronic media / storage devices.

f) Controls shall be implemented to prevent and detect any loss, damage, theft or compromise of the assets containing any Aadhaar related information.

g) The authentication devices used to capture resident's biometric shall be STQC certified Registered Devices. All the Sub-AUAs, Business Correspondents or other sub-contractors shall also use the STQC certified Registered Devices only.

h) Ownership of authentication assets shall be clearly defined and documented.

i) All the assets (e.g., POS devices, tablets, desktop, laptop, servers, databases etc.) used by **SPSPL** and its sub-contractors for Aadhaar Authentication shall be used after their hardening has been done as per the hardening baseline document. **SPSPL** shall define their own hardening standards, unless specified by UIDAI.

5. Access Control

a) Only authorized individuals shall be provided access to information facilities (such as Authentication application, audit logs, authentication servers, application, source code, information security infrastructure etc.) processing Aadhaar related information. Access Control List shall be maintained.

b) **SPSPL**, its sub-AUAs, BCs and other third-party personnel with access to UIDAI information assets shall have least privilege access for information access and processing.

c) 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.

d) Access rights and privileges to information facilities processing Aadhaar related information shall bereviewed on a quarterly basis and the report shall be maintained for audit purposes.

e) Common user IDs / group user IDs shall not be used. Exceptions shall be approved by **SPSPL** 's senior management and documented where there is no alternative.

f) Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems; if done manually, then a fire-proof safe or a password vault shall beused and an access log register shall be maintained.

g) The users shall not be provided with local admin access rights on their system. In the case of administrative access being provided, the users shall be prohibited from modifying the local securitysettings.

h) In the case of assisted devices and applications where operators need to mandatorily perform application functions (not a self-service application), operators should be authenticated using some authentication scheme such as password, Aadhaar authentication, smart card-based authentication, etc.

6. Password Policy

a) The allocation of initial passwords shall be done in a secure manner and these passwords shall bechanged at first login.

b) All user passwords (including administrator passwords) shall remain confidential and shall not beshared, posted or otherwise divulged in any manner.

c) If the passwords are being stored in the database or any other form, they should be stored in anencrypted / hashed form.

d) Password shall be changed whenever there is any indication of possible system or password compromise.

e) Complex passwords shall be selected with a minimum length of 8 characters, which:

(a) are not based on anything somebody else could easily guess or obtain using person relatedinformation, e.g. names, telephone numbers, and dates of birth etc.;

(b) is free of consecutive identical characters or all-numeric or all-alphabetical groups;

(c) contains at least one numeric, one uppercase letter, one lowercase letter and one specialcharacter;

(d) shall be changed at regular intervals (passwords for privileged accounts shall be changed morefrequently than normal passwords);

(e) shall not allow the use of last 5 passwords;

(f) shall not allow the username and password to be the same for a particular user;

(g) users shall not use the same password for various UIDAI access needs;

f) Password shall not be hardcoded in codes, login scripts, any executable program or files.

g) Password shall not be stored or transmitted in applications in clear text or in any reversible form.

h) Password shall not be included in any automated log-on process, e.g. stored in a macro or function key.

i) Three successive login failures shall result in user account being locked; they should not be able to login until their account is unlocked and the password reset. The user shall have to contact the System Engineers/Administrators for getting the account unlocked.

7. Cryptography and Security of Aadhaar number

a) The Personal Identity data (PID) block comprising of the resident's demographic / biometric data shallbe encrypted as per the latest API specifications rolled out by UIDAI.

b) The PID shall get encrypted at the end point device used for authentication and it shall remain encrypted during transit and flow within the ecosystem and while sharing this information with ASAs.

c) The encrypted PID block shall 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.

d) While providing authentication services to Sub-AUAs, **SPSPL** shall ensure that the client application used for Aadhaar authentication is developed and digitally signed by the **SPSPL**.

e) The key(s) used for digitally signing of authentication request and decryption of e-KYC XML Responseshall be stored in HSM only. The HSM used shall be FIPS 140-2 compliant.

f) All the HSM provisions shall be followed as defined in the circular – 11020/204/2017 dated 22nd June2017 and any subsequent guideline / circular / notice published by UIDAI in this regard.

g) The authentication request shall be digitally signed by **SPSPL** and/or by theAuthentication Service Agency, as per the mutual agreement between them.

h) Key management activities shall be performed by **SPSPL** to protect the keysthroughout their lifecycle. The activities shall address the following aspects of key management, including;

a) key generation;

b) key distribution;

c) Secure key storage;

d) key custodians and requirements for dual Control;

e) prevention of unauthorized substitution of keys;

f) Replacement of known compromised or suspected compromised keys;

g) Key revocation and logging and auditing of key management related activities.

i) The Reference Key used for Aadhaar Data Vault (ADV) should be generated using Universally UniqueIdentifier (UUID) scheme so that Aadhaar Number can neither be guessed nor reverse engineered using the reference.

j) 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 displaysshould be masked such that only last four digits of the Aadhaar number are displayed.

k) **SPSPL** shall make necessary changes in their authentication systems for useof Virtual token, UID token and Limited e-KYC.

l) **SPSPL** shall integrate Virtual Token and UID Token into their services.

8. Physical and Environmental Security

a) The servers should be placed in a secure cabinet in the **SPSPL's** Data Centre.

b) Data Centre hosting Aadhaar related information shall be fully secured and access controlled.

c) Data Centre shall be manned by security guards during and after office hours.

d) CCTV surveillance shall cover the AUA/KUA servers.

e) Access to the Data Centre shall be limited to authorized personnel only and appropriate logs for entryof personnel should be maintained.

f) The movement of all incoming and outgoing assets related to Aadhaar in the Data Centre shall bedocumented.

g) Lockable cabinets or safes shall be provided in the Data Centre and information processing facilitieshaving critical Aadhaar related information.

h) Fire doors and fire extinguishing systems shall be deployed, labelled, monitored, and tested regularly.

i) Preventive maintenance activities like audit of fire extinguishers, CCTV shall be conducted quarterly.

j) Physical access to Data Centre 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.

k) Signs or notices legibly setting forth the designation of restricted areas and provisions of entry shall beposted at all entrances and at other points along the restricted areas as necessary especially where theservers are physically hosted.

l) Controls shall be designed and implemented to protect power and network cables from unauthorized interception or damage.

m) A clear desk and clear screen policy for shall be adopted to reduce risks of unauthorized access, loss and damage to information related to Aadhaar. Screen saver or related technological controls shall beimplemented to lock the screen of the information systems when unattended beyond a specified duration.

n) Controls such as intrusion detection and evaluation plans shall be implemented in case of an

emergency.

9. Operations Security

a) **SPSPL** shall complete the Aadhaar on-boarding process as defined by UIDAI, before the commencement of formal operations.

b) Standard Operating Procedure (SOP) shall be developed for all information systems and services related to Aadhaar operations. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure.

c) 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.

d) 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.

e) **SPSPL's** 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.

f) The Test and Production facilities / environments shall be physically and/or logically separated.

g) A formal Patch Management Procedure shall be established for applying patches to the information systems. Patches should be updated at both application and server level.

h) Periodic Vulnerability Assessment (VA) exercise shall be conducted for ensuring the security of the Aadhaar infrastructure.

i) All hosts that connect to the Aadhaar Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. Anti-virus / malware detection software shall be installed on such hosts.

j) Network intrusion and prevention systems should be in place – e.g. IPS, IDS, WAF, etc.

k) Ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring.

l) Regular monitoring of the audit logs shall take place for any possible unauthorized use of information systems and results shall be recorded. Access to audit trails and event logs shall be provided to authorized personnel only.

m) The **SPSPL** shall follow all the consent related provisions as defined in the Aadhaar Act, 2016, Aadhaar Regulations 2016 and all circulars/notifications published from time to time.

n) The **SPSPL** shall maintain the logs of the Aadhaar authentication transaction as defined in the Aadhaar (Authentication) Regulations, 2016.

o) The Aadhaar authentication logs shall not, in any event, retain the PID information.

p) The e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, shall be stored in encrypted form after obtaining appropriate consent from the resident. Further, the usage of e-KYC data shall be governed as defined by the Aadhaar Act 2016, Aadhaar Regulations 2016 and all circulars/notifications published from time to time.

q) The e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, shall be shared with sub-AUA or any other entity after obtaining specific permission from UIDAI by submitting an application in this regard. After obtaining the appropriate permissions, the said data may be shared as per provisions of the Aadhaar Act, 2016, Aadhaar Regulations 2016 and all circulars/notifications published from time to time.

r) The client application used for Aadhaar authentication shall not store biometric data collected during authentication under any circumstances.

s) The logs of authentication transactions shall be maintained as defined by Aadhaar Act 2016, Aadhaar Regulations 2016 and all circulars/notifications published from time to time.

t) The server shall reside in a segregated network segment that is isolated from the rest of the network of the organisation. The server shall be dedicated for the online Aadhaar Authentication purposes and shall not be used for any other activities not related to Aadhaar.

u) All computer clocks shall be set to an agreed standard using a NTP server or shall be managed centrally and procedure shall be made to check for and correct any significant variation;

v) **SPSPL** or its sub-AUAs, BCs and other sub-contractors performing Aadhaar authentication shall ensure identity information is not displayed or disclosed to external agencies or unauthorized persons. Also, Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate or any other document/service shall not be published or displayed at any platform.

w) No data pertaining to the resident or the transaction shall be stored within the terminal device.

x) Aadhaar number and any other data kept in the Aadhaar Data Vault shall be kept in an encrypted format only.

y) **SPSPL** shall follow all the Aadhaar 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 this regard.

aa) **SPSPL** 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, Aadhaar number should not be linked with the biometric data collected for such other purposes.

bb) The user account shall be logged out after the session is finished.

cc) An auto lock out mechanism for workstation, servers and/ or network device shall be implemented.

dd) **SPSPL** shall not share its e-KYC license key with any other organisation. Sub- AUAs or any other entity shall not perform e-KYC using a **SPSPL**'s license key.

ee) 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.

ff) Separate license keys must be generated by **SPSL** for their Sub-AUAs in the manner prescribed by UIDAI.

gg) **SPSPL** must have its Aadhaar related servers hosted in data centres within India.

10. Communications security

a) Each authentication device shall have a Unique Device Code. This number shall be transmitted with each transaction along with UIDAI assigned institution code for **SPSPL** as specified by the latest UIDAI API documents.

b) A unique transaction number shall be generated automatically by the authentication device which should be incremented for each transaction processed.

c) The network between **SPSPL**, its sub-contractors and ASA shall be secure. **SPSPL** shall connect with ASAs through leased lines or similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shall be used.

d) The server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the server from all sources other than **SPSPL's** PoT terminals.

e) Use of web-based e-mail shall be restricted to official use and in accordance with the acceptable usage guidelines or as per organization policy.

11. Information Security Incident Management

a) **SPSPL** shall be responsible for reporting any security weaknesses, incidents, possible misuse or violation of any of the stipulated guidelines to UIDAI immediately.

b) **SPSPL** shall ensure that the sub-AUAs, BCs and other sub-contractors are aware about Aadhaar Authentication related incident reporting.

c) Root Cause Analysis (RCA) shall be performed for major Aadhaar related incidents identified in its as well as its sub-contractors' ecosystem.

d) Any confidentiality breach/security breach of Aadhaar related information shall be reported to UIDAI within 24 hours.

12. Compliance

a) **SPSPL** shall comply with the Aadhaar Act 2016, Aadhaar Regulations 2016, UIDAI agreement, as well as other notices and circulars published by UIDAI from time to time.

b) Application used for Aadhaar authentication shall be audited by information system auditor(s) certifiedby 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.

c) Permission shall be taken from UIDAI before appointment of an entity as their Sub-AUA. Also, **SPSPL** shall take permission for already appointed Sub-AUAs, if not done already.

d) **SPSPL** shall ensure that its operations and systems are audited by an information systems auditor certified by a recognised body on an annual basis to ensure compliance with UIDAI standards and specifications and the same shall be shared with UIDAI upon request.

e) In addition to the audits to be performed by **SPSPL** by itself on an annual basis, UIDAI may conduct audits of the operations and systems of **SPSPL**, either by itself or through an auditor appointed by UIDAI.

f) If any non-compliance is found as a result of the audit, management shall:

   a) Determine the causes of the non-compliance;

   b) Evaluate the need for actions to avoid recurrence of the same;

   c) Determine and enforce the implementation of corrective and preventive action;

   d) Review the corrective action taken.

g) **SPSPL** shall use only licensed software for Aadhaar related infrastructure environment. Record of all software licenses shall be kept and updated regularly.

h) **SPSPL** and its ecosystem partners shall ensure compliance to all the relevant laws, regulations as well as other notices, circulars and guidelines as defined by UIDAI from time to time.

i) Fraud Analytics module shall be deployed as part of its systems that is capable of analysing authentication related transactions to identify fraud.

j) **SPSPL** shall audit its Sub-AUAs, BCs or other sub-contractors providing Aadhaar Authentication services as per all the relevant laws, regulations as well as other notices, circulars and guidelines as defined by UIDAI from time to time.

k) For all authentication application deployed by **SPSPL** and its Sub-AUA, **SPSPL 's** logo shall be clearly visible.

13. Change Management

a) **SPSPL** shall document all changes to Aadhaar authentication applications, Infrastructure, processes and Information Processing facilities.

b) Change log/ register shall be maintained for all such changes performed.

***