


बिहार सरकार
मद्य निषेध, उत्पाद एवं निबंधन विभाग
अधिसूचना

पटना, दिनांक— 10.07.25

सं0सं0— FW-1725/15/2025-SEC_93849/ आधार (वित्तीय और सहायिकी लाभों और सेवाओं का लक्षित परिदान) अधिनियम, 2016 की धारा-4 की उपधारा (4) की कंडिका-ख की उप कंडिका-ii के तहत सह पठित सुशासन के लिए आधार अधिप्रमाणन (समाज कल्याण, नवाचार, ज्ञान) नियमावली, 2020 के नियम-05 बिहार मद्य निषेध एवं उत्पाद अधिनियम, 2016 की धारा-37 के अन्तर्गत बार-बार अपराध करने वाले व्यक्तियों को स्वैच्छिक आधार पर चिन्हित करने तथा निबंधन कार्यालयों में दस्तावेजों के निबंधन करने वाले इच्छुक पक्षकारों को चिन्हित करने के लिए आधार प्रमाणीकरण हेतु भारत सरकार द्वारा प्राधिकृत किये जाने के उपरान्त बिहार सरकार द्वारा विभाग को भी अधिकृत किया गया है। उक्त के आलोक में क्रमशः अधिसूचना संख्या-394, दिनांक-13.01.2023 एवं 2378, दिनांक-09.05.2023 निर्गत है।

अतः विभाग द्वारा आधार से संबंधित प्रमाणीकरण डाटा को संभालने वाले सभी सम्बद्ध एजेंसियों की पृष्ठ भूमि की जाँच एवं उनके कार्यों के संचालन हेतु सभी संबंधित बिन्दुओं यथा मानव संसाधन, परिसम्पत्ति प्रबंधन, पासवर्ड नीति, संचार सुरक्षा, व्यक्तिगत आँकड़ा संग्रहण आदि को ध्यान में रखते हुए विभागीय सूचना सुरक्षा नीति, 2025-26 (नीति की प्रति संलग्न) को अधिसूचित किया जाता है।

बिहार राज्यपाल के आदेश से,


(संजय कुमार)

सरकार के संयुक्त सचिव,


बिहार, पटना। 2/10.07.2025

ज्ञापांक— FW-1725/15/2025-SEC_93849

पटना, दिनांक— 10.07.25

प्रतिलिपि :—वित्त विभाग, ई-गजट कोषांग, बिहार, पटना को सी0डी0 सहित/अधीक्षक, राजकीय मुद्रणालय, गुलजारबाग, पटना-800007 को बिहार राजपत्र के आगामी अंक में प्रकाशनार्थ प्रेषित।

2. महालेखाकार, बिहार, वीरचन्द पटेल पथ, पटना को सूचनार्थ एवं आवश्यक कार्रवाई हेतु प्रेषित।
3. सचिव, सूचना प्रावैधिकी विभाग, बिहार, पटना/प्रबंध निदेशक, बेल्लूॉन, शास्त्रीनगर, पटना को सूचनार्थ प्रेषित।
4. माननीय मंत्री के आप्त सचिव को सूचनार्थ प्रेषित।
5. सचिव के आप्त सचिव/आयुक्त उत्पाद-सह-निबंधन महानिरीक्षक के आप्त सचिव को सूचनार्थ प्रेषित।
6. सभी समाहर्ता/सभी उपायुक्त मद्यनिषेध/सभी सहायक निबंधन महानिरीक्षक/सभी सहायक आयुक्त मद्यनिषेध/सभी जिला अवर निबंधक/सभी अधीक्षक मद्यनिषेध/सभी अवर निबंधक को सूचनार्थ प्रेषित।
7. सभी विभागीय पदाधिकारी (मुख्यालय) को सूचनार्थ प्रेषित।
8. विभागीय आई0टी0 मैनेजर को विभागीय वेबसाईट पर अपलोड करने हेतु प्रेषित।


सरकार के संयुक्त सचिव,
बिहार, पटना।

2/10.07.2025

Prohibition, Excise and Registration Department,

Govt. of Bihar



Information Security Policy

2025-26

Version 1.0

82 & 2nd 0

Scope

This is with reference to the Aadhaar Authentication Services of Unique Identification Authority of India (UIDAI) for the stakeholders of Prohibition, excise and registration department (PERD), Registration Management System (hereinafter referred to as "PERD" or "Sub AUA").

This document outlines the Information Security Policy and standards applicable to PERD and its stakeholders in their role as a Sub-Aadhaar Authentication User Agency (Sub-AUA).

Document distribution

All Employees of PERD including Registered Workers, PERD Stakeholders and third parties who access information through PERD information system or handle any information Asset of PERD related to Aadhaar.

DOCUMENT CONTROL

Title	Information Security Policy	Version No	1.0
Created by	Shri. Sunil Kumar, IT Manager	Date	27-06-2025
Reviewed by	Shri Sushil Kumar Suman, DIG (Reg.) Smt. Renu Kumari sinha, Dy.Comm. (Excise)	Date	30-06-2025
Approved by	Shri Ajay Yadav, Secretary	Date	01-07-2025

VERSION CONTROL

Version	Effective From	Type of Change	Approved By
1.0	09-07-2025	First Version	Shri Ajay Yadav, Secretary

8 & 8 2025

Aadhaar Information Security Policy

Contents

Terms & Definitions.....	3
1. About the Policy.....	5
1.1 Policy Statement	5
1.2 Policy Scope	5
2 Information Security Domains and related Controls	6
2.1 Human Resources.....	6
2.2 Asset Management.....	6
2.3 Access Control.....	6
2.4 Password Policy.....	7
2.5 Cryptography.....	8
2.6 Operations Security	8
2.7 Communications security	9
2.8 Information Security Incident Management.....	10
2.9 Personal Data Collection.....	11
2.10 Specific purpose for collection of Personal data.....	11
2.11 Obtaining Consent.....	11
2.12 Personal Data Protection	12
2.13 Sharing of Personal data	12
2.14 Retention of Personal Data	12
2.15 Data Backup Policy	12
2.16 Data Privacy on Aadhaar and Biometric Details	13
3 Third party access and Outsourcing	13
4 Risk Assessment and security auditing requirements.....	14
5 Change Management	15

[Handwritten signature] *[Handwritten signature]* *[Handwritten signature]* *[Handwritten signature]* *[Handwritten signature]*

Terms & Definitions

S. No.	Terms	Definition
1	AAS	AADHAAR Authentication Server
2	API	Application Program Interface
3	AUA/ASA	Authentication User Agency/Authentication Service Agency
4	Sub-AUA	Sub Authentication User Agency
5	CA	Certifying Authority
6	CIDR	Central Identities Data Repository
7	CN	Common Name
8	Asset	<p>An asset is anything that has value to the organization. Assets can be classified into the following 5 categories:</p> <ol style="list-style-type: none"> 1. Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) 2. Physical assets: (computer equipment, communications, utility equipment, buildings etc.) 3. Software assets: (database information, applications, software code, development tools, operational software etc.) 4. People assets: UIDAI human resources and stakeholders. 5. Service assets: (Logistics, building management systems, communications, utilities etc.)
9	Information/ Information Asset (IA)	Information that has value to the organization (UIDAI). Including but not limited to Citizen biometric and demographic information, personally identifiable information, employee information, organization information such as CIDR details etc.
10	IT	Information Technology
11	KUA	Know your customer User Agency
12	NDA	Non-Disclosure Agreement
13	NTP	Network Time Protocol
14	OTP	One Time Password
15	PID	Personal Identity Data
16	SOP	Standard Operating Procedures
17	SPOC	Single Point of Contact

Handwritten signatures and initials.

18	SSL	Secure Sockets Layer
19	STQC	Standard Testing and Quality Control
20	VA	Vulnerability Assessment
21	VPN	Virtual Private Network
22	PERD	Prohibition, Excise and Registration Department

g r & p u s (3)

1. About the Policy

1.1 Policy Statement

Security of UIDAI Information Assets handled by the PERD for providing services is of paramount importance. PERD and its stakeholders shall ensure the confidentiality, integrity, and availability of these at all times by deploying suitable controls commensurate with the asset value and in accordance with applicable rules.

1.2 Policy Scope

This Aadhaar Information Security Policy is applicable wherever UIDAI information is processed and/or stored by all Stakeholders, PERD and its Sub-AUAs. The policy may be amended from time to time as per regulations of UIDAI.

g. l. b. p. r. f. ①

2 Information Security Domains and related Controls

2.1 Human Resources

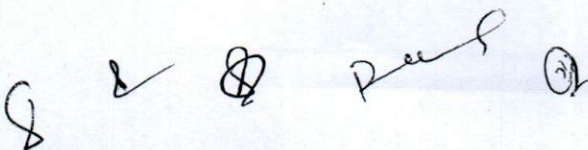
1. PERD shall appoint a MPoC and TPoC for Aadhaar related activities and communication with UIDAI;
2. PERD shall conduct a background check or sign an agreement/NDA with all personnel/agency handling Aadhaar related authentication data. UIDAI or agency appointed by UIDAI may validate this information.
3. Induction as well as periodic functional and information security trainings shall be conducted for all PERD personnel for Aadhaar related authentication services. The training shall include all relevant security guidelines as per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
4. All employees and third party service providers accessing UIDAI Information Assets shall be made aware of UIDAI information security policy and controls.

2.2 Asset Management

5. All Assets used by the PERD (As defined in 1.1 above) for the purpose of delivering services to Registration employee using Aadhaar authentication services shall be identified labelled and classified. Details of the Information Assets shall be recorded.
6. The assets which are scheduled to be disposed shall be disposed as per PERD's Information Security Policy;
7. Before sending any equipment out for repair, the equipment shall be sanitized to ensure that it does not contain any UIDAI sensitive data;
8. Sub-AUA shall not transfer or make an unauthorized copy of any identity information from removable media to any personal device or other unauthorized electronic media / storage devices.
9. Sub-AUA shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.
10. Authentication devices used to capture residents' biometric shall be STQC certified as specified by UIDAI.

2.3 Access Control

1. 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 UIDAI information;
2. PERD employees and third party service providers with access to UIDAI information assets shall:
 - a) Have least privilege access for information access and processing;
 - b) The operator must be logged out after the session is finished.
 - c) Implement an equipment locking mechanism for workstation, servers and/ or network device



3. The application should have auto log out feature i.e. after a certain time of inactivity (15 mins or as specified in the UIDAI Authentication Regulations document), the application should logout.
4. Access rights and privileges to information processing facilities for UIDAI information shall be revoked within 24 hours separation of respective personnel or as mentioned in the exit management policy of the organization Post deactivation, user IDs shall be deleted if not in use as per Exit formalities.
5. Access rights and privileges to information facilities processing UIDAI information shall be reviewed on a quarterly basis and the report shall be stored for audit purposes;
6. Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approved and documented where there is no alternative;
7. Procedures shall be put in place for secure storage and management of administrative passwords for critical information systems. If done manually, then a fireproof safe or similar password vault must be used to maintain the access log register.
8. The users should 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 security settings. Modifying the same shall result in disciplinary action.
9. Three successive login failures or as per the access control policy/password policy of the organization should result in a user's account being locked; they should not be able to login until their account is unlocked and the password reset in case of server logins. The user should contact the System Engineers/Administrators for getting the account unlocked. For applications, there should be an automatic lock out period of 30 mins in case of three consecutive login failures or as per the access control policy/password policy of the organization.
10. If the application is operator assisted, the operator shall first confirm his identity by authenticating himself before authenticating the residents.
11. The access rules of firewalls shall be maintained only by users responsible for firewall administration.

2.4 Password Policy

1. The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login;
2. All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted, or otherwise divulged in any manner;
3. Keeping a paper record of passwords shall be avoided, unless this can be stored securely;
4. If the passwords are being stored in the database or any other form, they should be stored in encrypted form.
5. Passwords shall be changed whenever there is any indication of possible system or password compromise;

[Handwritten signatures and initials]

2.5 Cryptography

1. The Personal Identity data (PID) block comprising of the resident's demographic+ /biometric data shall be encrypted as per the latest API documents specified by the UIDAI at the end point device used for authentication.
2. The PID shall be encrypted during transit and flow within the AUA ecosystem and while sharing this information with ASAs; Logs of the authentication transactions shall be maintained but PID Information shall not be retained.
3. The encrypted PID block should 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;

2.6 Operations Security

1. PERD shall complete the AADHAAR Sub AUA on-boarding process before the commencement of formal operations;
2. Standard Operating Procedure (SOP) shall be developed for all information systems and services related to UIDAI 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;
3. Persons 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;
4. 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;
5. The Test and Production facilities-environments must be physically and/or logically separated.
6. The Operating System as well as the network services used for communication shall be updated with the latest security patches.
7. 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;
8. Periodic VA exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.
9. PERD employees 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 PID information;
10. All hosts that connect to the AADHAAR Authentication Service information shall be secured using endpoint security solutions. At the minimum, anti-virus-malware detection software shall be

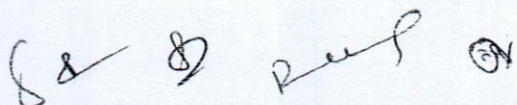
[Handwritten signatures and initials]

installed on such hosts;

11. PERD / System Integrator (SI) shall ensure that the event logs are to be recorded and stored to assist in future investigations and access control monitoring;
12. 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;
13. The authentication audit logs should contain, but not limited to, the following transactional details:
 - a) Aadhaar Number against which authentication is sought;
 - b) Specified parameters of authentication request submitted;
 - c) Specified parameters received as authentication response;
 - d) The record of disclosure of information to the Aadhaar number holder at the time of authentication
 - e) Record of the consent of Aadhaar number holder for the resident
 - f) Details of the authentication transaction such as API Name, AUA / KUA Code, Sub-AUA, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-identity information.
14. Network intrusion and prevention systems should be in place;
15. Logs shall not, in any event, retain the PID, biometric and OTP information;
16. The logs of authentication transactions shall be maintained by PERD for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified;
17. Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years or the number of years as required by the laws or regulations of Govt. of India, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes;
18. All computer clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation;
19. The Sub AUA server host shall reside in a segregated network segment that is isolated from the rest of the network of the PERD; The AUA server host shall be dedicated for the Online AADHAAR Authentication purposes and shall not be used for any other activities;

2.7 Communications security

1. In case of a composite terminal device that comprises of a biometric reader without embedded software to affect the encryption of the personal identity data, communication between the biometric reader and the device performing the encryption shall be secured against all security



threats / attacks

2. Terminal devices shall provide different logins for operators. These users shall be authenticated using some additional authentication scheme such as passwords, AADHAAR authentication, etc.;
3. Each terminal shall have a unique terminal ID. This number must be transmitted with each transaction along with UIDAI assigned institution code for the AUA as specified by the latest UIDAI API documents
4. A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transaction processed;
5. The Sub AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA server from all sources;
6. Special consideration shall be given to Wireless networks due to poorly defined network perimeter. Appropriate authentication, encryption and user level network access control technologies shall be implemented to secure access to the network;
7. 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;

2.8 Information Security Incident Management

1. PERD shall be responsible for reporting any security weaknesses, any incidents, possible misuse, or violation of any of the stipulated guidelines to UIDAI immediately.
2. PERD shall ensure that its employees, BCs and other sub-contractors are aware about Aadhaar Authentication related incident reporting.
3. Root Cause Analysis (RCA) shall be performed for major Aadhaar related incidents identified in its as well as its sub-contractors' ecosystem.
4. Any confidentiality breach/security breach of Aadhaar related information shall be reported to UIDAI within 24 hours.
5. From the effective date of sub-section (6) of section 8 of the DPDP Act, report any personal data breach to the Data Protection Board and notify each affected individual within the time specified by the Act's rules.
6. Contact Details for Reporting and Escalation:

Prohibition, excise and Registration Department, Govt. of Bihar

DIG, Registration

Email: excise-bih@nic.in

Phone: +91 91100 36303

Address: First Floor, Vikas Bhawan Patna- 800015

2.9 Personal Data collection

[Handwritten signatures and initials]

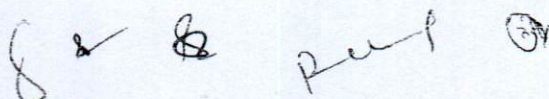
1. PERD shall collect the personal data including Aadhaar number/Virtual ID, directly from the Aadhaar number holder for conducting authentication with UIDAI at the time of providing the services;

2.10 Specific purpose for collection of Personal data

1. The Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide scheme Benefits.
2. The identity information collected and processed shall only be used pursuant to applicable law and as permitted under the Aadhaar Act 2016 or its Amendment and Regulations.
3. The identity information shall not be used beyond the mentioned purpose without consent from the Aadhaar number holder and even with consent use of such information for other purposes should be under the permissible purposes in compliance to the Aadhaar Act 2016.
4. Process shall be implemented to ensure that Identity information is not used beyond the purposes mentioned in the notice/consent form provided to the Aadhaar number holder.
5. Notice / Disclosure of Information to Aadhaar number holder
6. Aadhaar number holder shall be provided relevant information prior to collection of identity information / personal data. These shall include:
 - i) The purpose for which personal data / identity information is being collected;
 - ii) The information that shall be returned by UIDAI upon authentication;
 - iii) The information that the submission of Aadhaar number or the proof of Aadhaar is mandatory or voluntary for the specified purpose and if mandatory the legal provision mandating it;
 - iv) The alternatives to submission of identity information (if applicable);
 - v) Details of Section 7 notification (if applicable) by the respective department under the Aadhaar Act, 2016, which makes submission of Aadhaar number as a mandatory or necessary condition to receive subsidy, benefit or services where the expenditure is incurred from the Consolidated Fund of India or Consolidated Fund of State. Alternate and viable means of identification for delivery of the subsidy, benefit or service may be provided if an Aadhaar number is not assigned to an individual;
 - vi) The information that Virtual ID can be used in lieu of Aadhaar number at the time of Authentication;
 - vii) Aadhaar number holder shall be notified of the authentication either through the e-mail or phone or SMS at the time of authentication and the PERD shall maintain logs of the same;

2.11 Obtaining Consent

1. Upon notice / disclosure of information to the Aadhaar number holder, consent shall be taken in writing or in electronic form on the website or mobile application or other appropriate means and



PERD shall maintain logs of disclosure of information and Aadhaar number holder's consent.

2. Legal department shall be involved in vetting the method of taking consent and logging of the same, and formal approval shall be recorded from the legal department;

2.12 Personal Data Protection

1. Aadhaar authentication or Aadhaar e-KYC shall be used for the specific purposes declared to UIDAI and permitted by UIDAI. Such specific purposes shall be notified to the residents / customers / Individuals at the time of authentication through disclosure of information notice;
2. PERD shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under Aadhaar Act 2016 and its associated Regulation and informed to the resident / customers / individuals at the time of Authentication.
3. For the purpose of e-KYC, the demographic details of the individual received from UIDAI as a response shall be used for identification of the individual for the specific purposes of providing the specific services for the duration of the services.
4. Data Protection related aspects under the Aadhaar Act, the regulation made thereunder and the standards and specifications issued by UIDAI and other regulatory authorities from time to time shall be adhered.

2.13 Sharing of Personal data

1. Identity information shall not be shared in contravention to the Aadhaar Act 2016, its Amendment, Regulations and other circulars released by UIDAI from time to time.
2. Biometric information collected shall not be transmitted over any network without creation of encrypted PID block as per Aadhaar Act and regulations;

2.14 Retention of Personal Data

The authentication transaction logs shall be stored for a period of two years subsequent to which the logs shall be archived for a period of five years or as per the regulations governing the entity, whichever is later and upon expiry of which period, barring the authentication transaction logs required to be maintained by a court order or pending dispute, the authentication transaction logs shall be deleted.

2.15 Data Backup Policy

- a) Back-up procedures should be documented, scheduled and monitored.
- b) Up-to-date backups of all critical items should be maintained to ensure the continued provision of the minimum essential level of service. These items include:

- Data files
- Utilities programs
- Databases
- Operating system software
- Applications system software



- Encryption keys
- Pre-printed forms
- Device configurations

- c) One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.
- d) Backups of the system, application and data should be performed on a regular basis as per the DR and BCP policy of the Bihar State Data Centre.

2.16 Data Privacy on Aadhaar and Biometric details

1. The submission of Aadhaar details by a construction worker to the PERD is voluntary and the PERD shall not insist on a worker to produce their Aadhaar details for availing any of the services. In cases where Aadhaar number is offered voluntarily by the customer to the PERD, the department shall seek a declaration by the customer towards the same.
2. For cases where e-KYC verification is required, the PERD shall get an explicit consent from the worker for download of resident demographic details from UIDAI mentioning the purpose for which the details are sought.
3. The consent shall be either in the form of an authorization letter or a provision to electronically record the consent in a software application.
4. The biometric details whenever captured by the PERD shall be used only for data exchange with UIDAI which validates the captured biometric data against the biometric data maintained in CIDR (Central Identities Data Repository) against the specific Aadhaar number.
5. PERD shall use STQC certified devices for demographic details received from UIDAI will be stored for future reference, the biometric details shall not be stored by the PERD in any manner and form.
6. A system log wherever required shall be maintained to extract the details in case of disputes. The logs should capture Aadhaar Number, timestamp etc., but will not capture/store the PID (Personal Identity Data) associated with the transaction.
7. The data so captured will be sent to UIDAI as a straight through process. PERD shall not store the data captured (both biometric and personal information) in any manner and form.

3. Third party access and Outsourcing

- 3.1 PERD shall ensure that third party access to information should be restricted and should only be shared after signing Non-Disclosure-Agreement.
- 3.2 Wherever any activity is outsourced or awarded as work contract to any 3rd party / vendor, it shall be ensured that the contract specifies the information security requirements, and the same are complied with, in addition to the regular contractual details.
- 3.3 The following information security requirements should be documented as part of the contract:
 - i. General policy on information security.
 - ii. Procedures to protect organisational assets.

[Handwritten signatures and initials]

- iii. Restrictions on copying / disclosure.
- iv. Controls to ensure return of information/assets in their possession at the end of the contract.
- v. The right to monitor and the right to terminate services in the event of a security incident or a security breach.
- vi. Right to audit contractual responsibilities or to have the audits carried out by third parties.
- vii. Arrangements for reporting, notification and investigation of security incidents and breaches.

3.4 Information security audit report of the vendor to be made available to Procuring entity on periodic basis or when required.

3.5 Detailed list of all components of the software (including open source) / solution in the form of Software Bill Of Material (SBOM) shall be provided by the vendor. Vendor is also responsible for informing any identified vulnerabilities in the system to the organisation within reasonable time period.

3.6 Data collected and processed by the vendor should be protected appropriately (cannot be shared with any others without explicit consent / agreement) and made available to the procuring entity as and when required. External party personnel should comply with the information security policies, processes and procedures of the organisation.

3.7 Any external party found in violation to this policy shall be subjected to termination of contract and/ or will be handled as per applicable laws, rules & regulations.

4. Risk Assessment and security auditing requirements:

4.1 PERD must hold meetings with all stakeholders and heads of the department to chalk out the requirements for security audits such as the following:

- i. Scope of the audit
- ii. Risk based asset classification
- iii. Audit benchmarks, standards and compliance requirements
- iv. Remediation plan on audit findings
- v. Audit report format along with requirements of evidence and artifacts
- vi. Follow-up audits
- vii. Examine the effectiveness of the existing policy, standards, guidelines and procedures

4.2 Periodicity and nature of audits

- i. Internal information security audit to be performed at least once in a year.
- ii. 3rd Party Security audits must be conducted periodically at least once a year to ensure compliance with security policy, guidelines, and

Handwritten signatures and initials at the bottom of the page.

procedures, and to determine the minimum set of controls required to address PERD's security.

- iii. Security audit should be performed prior to and after implementation or installation or major enhancements in the PERD
- iv. Follow-up audits should be conducted to ensure compliance and closure of vulnerabilities

5. Change Management

- i. All changes to UIDAI Information Processing facilities/ Infrastructure/ processes shall be documented.
- ii. Only those changes related to Aadhaar which are approved by UIDAI for execution shall be implemented.
- iii. Change log/ register shall be maintained for all changes performed.

-----End of Document-----

✓ 82 Ref 04