## Data Privacy Policy

The purpose of Data Privacy policy is to maintain the privacy and protect the personal information of employees, contractors, vendors, interns, associates, customers, and business partners of MAFIL and ensure compliance with laws and regulations applicable to MAFIL.

This policy explains which personal data concerning the Data Personnel shall be collected, when he/she shall share the data to the organizations, when and why the organization collect the personal data, how the organization use the personal data, the conditions of the organizations disclosure to third parties, as well as how the organization secure the stored personal data.

* 1. *Policy Coverage*

Data Privacy Policy shall be applicable to all MAFIL employees, contractors, vendors, interns, associates, customers, and business partners who receive personal information from MAFIL, who have access to personal information collected or processed by MAFIL, or who provides information to MAFIL, regardless of geographic location.

All employees of MAFIL shall support the privacy policy and principles when they collect and / or handle personal information and / or involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization’s commitment towards data privacy.

All partner firms and any Third-Party working with or for MAFIL, and who have or may have access to personal information shall read, understand and comply with this policy. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

**18 |** P a g e Information Security Policy Version 1.4 Confidential

* **Collection** - MAFIL shall collect personal information only for the purposes identified in the notice.
* **Use, retention, and disposal** - MAFIL shall limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. MAFIL shall retain personal information only as long as it is necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
* **Access** - MAFIL shall provide individuals with access to their personal information for review and update.
* **Disclosure to third parties** - MAFIL shall disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
* **Security for privacy** - MAFIL shall protect personal information against unauthorized access (both physical and logical).
* **Quality** - MAFIL shall maintain accurate, complete, and relevant personal information for the purposes identified in the notice.
* **Monitoring and enforcement** - MAFIL shall monitor compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

*5.4 Notice*

Notice shall be made readily accessible and available to data subjects before or at the time of collection of personal information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously and shall be provided online (e.g. by posting it on the website/intranet portal/mobile applications) and/or offline methods (e.g. through posts, couriers, etc.).

Manappuram Finance Limited Confidential P a g e | **19**

information to be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and will be disposed-off securely or made anonymous post the identified purpose is completed.

* process of accessing personal information; the costs associated for accessing personal information (if any); process to update / correct the personal information; the resolution of disagreements related to personal information.
* how the information is protected from unauthorized access or use.
* how users will be notified of any changes made to privacy notice;
* disclosure process for Third Parties; the assurance that the personal information is disclosed to Third Parties only for the purpose identified; the remedial actions in place for any misuse of personal information by the Third Parties.
* security measures in place to protect personal information; ways of maintaining quality of personal information.
* monitoring and enforcement mechanisms in place; description of the complaint channels available to data subjects; how the internal personnel, key stakeholders and the customers can contact the organization related to any privacy complaints or breaches; relevant contact information and/or other reporting methods through which the complaints and/or breaches could be registered.
* Consequences of not providing the requested information.

*5.5 Choice and consent*

Choice refers to the options for the data subjects are offered regarding the collection and use of their personal information. Consent refers to their agreement to the collection and use, often expressed by the way in which they exercise a choice option.

Manappuram Finance Limited Confidential P a g e | **20**

privacy protection shall apply to all personal information.

* Personal information shall not be collected unless either of the following is fulfilled:
  + The data subject has provided valid, informed and free consent.
  + processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
  + processing is necessary for compliance with the organization’s legal obligation.
  + processing is necessary in order to protect the vital interests of the data subject.
  + processing is necessary for the performance of a task carried out in the public interest
* Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible.
* Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost.
* When using vendors to collect personal information on the behalf of MAFIL, it shall ensure that the vendors comply with the privacy requirements of MAFIL as defined in this policy.
* MAFIL shall at minimum, annually review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose.
* Respective department/function shall obtain approval from the CTO and CISO before adopting the new methods for collecting personal information electronically.

Manappuram Finance Limited Confidential P a g e | **21**

MAFIL has the right to retain the personnel information for legal and regulatory purposes and as per

applicable data privacy laws.

* MAFIL shall perform an internal audit on an annual basis to ensure that personal information collected is

used, retained and disposed of in compliance with the organization’s data privacy policy.

*5.8 Access*

MAFIL shall establish a mechanism to enable and facilitate exercise of data subject’s rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal information.

* Data subjects shall be entitled to obtain the details about their own personal information upon a request made and set forth in writing. MAFIL shall provide its response to a request within 72 hours of receipt of written request.
* The data subjects shall have the right to require MAFIL to correct or supplement erroneous, misleading, outdated, or incomplete personal information.
* Requests for access to or rectification of personal information shall be directed at the data subject’s option, to the respective head of department of the projects team or support function responsible for the personal information.
* The privacy coordinators shall record and document each access request as it is received, and the corresponding action taken.
* MAFIL shall provide personal information to the data subjects in a plain simple format which is understandable.

Manappuram Finance Limited Confidential P a g e | **22**

Information security policy and procedures shall be documented and implemented to ensure reasonable security for

personal information collected, stored, used, transferred and disposed by MAFIL

* Information asset labelling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.
* MAFIL shall establish procedures that maintain the logical and physical security of personal information.
* MAFIL shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
* Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.
* Individuals noticing or becoming aware of any breach of personal data shall notify the DPO (email at [ciso@manappuram.com)](mailto:ciso@manappuram.com) within 2 hours. It shall be the DPO’s responsibility to analyze and act on the intimation of the same within 48 hours.

# 5.11 Quality

MAFIL shall maintain data integrity and quality, as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete and current.

* For this purpose, the nodal/data protection officer shall have systems and procedures in place to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
* MAFIL internal audit department shall perform an annual assessment on the personal information collected to check for accuracy, completeness and relevance of the personal information.

Manappuram Finance Limited Confidential P a g e | **23**

the attention of the Grievance Officer whose details are as mentioned below.

|  |  |
| --- | --- |
| Name | YOGEESHA P |
| Contact Number | 8320718210 |
| E-mail | [headcrm@manappuram.com](mailto:headcrm@manappuram.com) |
| Working Days / Hours | Monday to Friday / 8:30 am to 5:30 pm |

5.13

*Dispute Resolution and Escalation Process for Customer / Third Party*

Customers / Third Party with inquiries or complaints about the processing of their personal information shall bring the matter to the attention of the Grievance Officer in writing. Any disputes concerning the processing of the personal information of non-employees shall be resolved through arbitration.

# 5.14 Compliance Review

Internal audit team shall conduct an internal audit annually (at minimum) to ensure compliance with the established privacy policies and applicable laws.

* The internal audit shall consist of the review of the following:
  + personal information collected from data subjects.
  + the purposes of the data collection and processing.
  + the actual uses of the data.
  + disclosures made about the purposes of the collection and use of such data.
  + The existence and scope of any data subject consents to such activities.

Manappuram Finance Limited Confidential P a g e | **24**

1. Legal Framework
   * The policy is guided by the provisions of the Aadhaar Act and regulations made thereunder, including any standards and specifications mandated by UIDAI.
   * It also adheres to relevant provisions of the Information Technology Act and other applicable laws and regulations governing data protection in India.
2. Data Protection Principles
   * Lawfulness, Fairness, and Transparency: All processing of Aadhaar data shall be conducted lawfully, fairly, and transparently, with explicit consent obtained from individuals where required.
   * Purpose Limitation: Aadhaar data shall be collected, processed, and used only for specific, legitimate purposes disclosed to individuals.
   * Data Minimization: Only the minimum necessary Aadhaar data required for the intended purpose shall be collected and retained.
   * Accuracy and Integrity: Adequate measures shall be taken to ensure the accuracy and integrity of Aadhaar data throughout its lifecycle.
   * Confidentiality and Security: Adequate technical and organizational measures shall be implemented to safeguard Aadhaar data against unauthorized access, disclosure, alteration, or destruction.
   * Accountability: The organization shall be accountable for compliance with legal requirements and shall ensure that individuals' rights regarding their Aadhaar data are respected.
3. Roles and Responsibilities
   * Transmission: Adequate encryption and other security measures shall be employed to protect Aadhaar data during transmission.
   * Disposal: Aadhaar data shall be securely deleted or anonymized when it is no longer needed for the purpose for which it was collected.
4. Training and Awareness
   * All employees shall receive training on data protection principles, procedures, and their roles and responsibilities under this policy.
   * Regular awareness programs shall be conducted to ensure that employees remain informed about updates to data protection laws and best practices.
5. Monitoring and Enforcement
   * Regular audits and assessments shall be conducted to monitor compliance with the data protection policy.
   * Non-compliance with the policy shall result in disciplinary action, up to and including termination of employment or contractual relationship.
6. Review and Update
   * This policy shall be reviewed periodically to ensure its effectiveness and compliance with evolving legal and regulatory requirements.
   * Updates to the policy shall be communicated to all relevant stakeholders.
7. Documentation and Records Management

This Data Protection Policy provides a framework for the secure handling of Aadhaar data, ensuring

compliance with legal and regulatory requirements while maintaining the trust and confidence of individuals whose data is being processed.

5.16 Aadhar Data Privacy Policy

# Terms and Definitions:

* “***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*
* “***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*
* "***Anonymization***" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which an individual cannot be identified, which meets the standards of reversibility.
  + *Reference: Section 3 (2) of the Personal Data Protection Bill 2019*
* “***Authentication***” means the process by which the Aadhaar number along with demographic

*(Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016*

* “***Biometric information***” means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.
  + *Reference: Section 2(g) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016*
* “***Central Identities Data Repository***” (**CIDR**) means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto.
  + *Reference: Section 2(h) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016*
* “***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.
  + The consent of the data principal shall not be valid, unless such consent is—

free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;informed, having regard to whether the data principal has been provided with the information required under section 7;

specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

* + 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.
* ***“De-identification”*** means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;
  + *Reference: Section 3(16) of the Personal Data Protection bill 2019*
* “***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*
* “***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.
  + *Reference: Regulation number 2(l) of the Aadhaar (Authentication) Regulations, 2016*
* “***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*
  + *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*

* “***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*
* ***“Personal data”*** means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;
  + *Reference: Section 3(28) of the Personal Data Protection bill 2019*
* ***“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*
* ***"Processing"*** in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;
  + *Reference: Section 3(31) of the Personal Data Protection bill 2019*
    - password;
    - financial information such as Bank account or credit card or debit card or other payment instrument details;
    - physical, physiological and mental health condition;
    - sexual orientation;
    - medical records and history;
    - Biometric information;
    - any detail relating to the above clauses as provided to body corporate for providing service; and
    - 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*
* “***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

thereunder.

# Personal Data collection

* + a. Manappuram Finance Limited shall collect the personal data including Aadhaar number/Virtual ID, directly from the Aadhaar number holder for conducting authentication with UIDAI at the timeof providing the services;

# Specific purpose for collection of Personal data

* The Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide e-KYC
* 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.
* 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.
* 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
  + The information that Virtual ID can be used in lieu of Aadhaar number at the time of Authentication;
  + The name and address of the Manappuram Finance Limited collecting and processing the personal data;
* 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 Manappuram Finance Limited shall maintain logs of the same;

# Obtaining Consent

* 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 Manappuram Finance Limited shall maintain logs of disclosure of information and Aadhaar number holder’s consent.
* 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;

# Processing of Personal data

* The identity information, including Aadhaar number, biometric /demographic information collected from the Aadhaar number holder by Manappuram Finance Limited shall only be used for the Aadhaar authentication process by submitting it to the Central Identities Data Repository (CIDR).

# Sharing of Personal data

* 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.
* Biometric information collected shall not be transmitted over any network without creation of encrypted PID block as per Aadhaar Act and regulations;
* Manappuram Finance Limited shall not require an individual to transmit the Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances;

# Data Security

* The Aadhaar number shall be collected over a secure application, transmitted over a secure channel as per specifications of UIDAI. The information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential and secure.
* The biometric information shall be collected, if applicable, using the registered devices specified by UIDAI. These devices encrypt the biometric information at device level and the application sends the same over a secure channel to UIDAI for authentication.
* OTP information shall be collected in a secure application and encrypted on the client device before transmitting it over a secure channel as per UIDAI specifications;

the processing of Identity information; The applications shall be audited on an annual basis

by information systems auditor(s) certified by STQC, CERT-IN or any other UIDAI recognized body;

* In the event of an identity information breach, the organisation shall notify UIDAI within 72 hours after having knowledge of misuse of any information related to the Aadhaar related information or system with the following :
  + A description and the consequences of the breach;
  + A description of the number of Aadhaar number holders affected and the number of records affected;
  + The privacy officer’s contact details;
  + Measures taken to mitigate the identity information breach;
* Appropriate security and confidentiality obligations shall be implemented in the non- disclosure agreements (NDAs) with employees/contractual agencies /consultants/advisors and other personnel handling identity information;
* Only authorized individuals shall be allowed to access Authentication application, audit logs, authentication servers, application, source code, information security infrastructure. An access control list shall be maintained and regularly updated by organisation;
* Best practices in data privacy and data protection based on international Standards shall be adopted;
* The response received from CIDR in the form of authentication transaction logs shall be stored with following details:
* The Aadhaar number holder has the right to obtain and request update of identity

information stored with the organisation, including Authentication logs. The collection of core biometric information, storage and further sharing is protected by Section 29 of the Aadhaar Act 2016, hence the Aadhaar number holder cannot request for the core biometric information.

* Manappuram Finance Limited shall provide a process for the Aadhaar number holder to view their identity information stored and request subsequent updation after authenticating the identity of the Aadhaar number holder. In case the update is required from UIDAI, same shall be informed to the Aadhaar number holder.
* The Aadhaar number holder may, at any time, revoke consent given to Manappuram Finance Limited for storing his e-KYC data, and upon such revocation, Manappuram Finance Limited shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.
* The Aadhaar number holder has the right to lodge a complaint with the privacy officer who is responsible for monitoring of the identity information processing activities so that the processing is not in contravention of the law;

# Aadhaar Number Holder Access request

* A process shall be formulated to handle the queries and process the exercise of rights of Aadhaar number holders with respect to their identity information / personal data. As part of the process it shall be mandatory to authenticate the identity of the Aadhaar number holder before providing access to any identity information.
* All requests from the Aadhaar number holder shall be formally recorded and responded to within a reasonable period.

identification and minimization shall be implemented to make the collection of identity

information adequate, relevant, and limited to the purpose of processing.

# Governance and Accountability Obligations

* A Privacy committee shall be established to provide strategic direction on Privacy matters
* A person (Privacy Officer) responsible for developing, implementing, maintaining and monitoring the comprehensive, organization-wide governance and accountability shall be designated to ensure compliance with the applicable laws.
* The name of the Privacy Officer and contact details shall be made available to UIDAI and other external agencies through appropriate channel;
* The Privacy Officer shall be responsible to assess privacy risks of processing Identity information / personal data and mitigate the risks;
* The Privacy Officer shall be independent and shall be involved in all the issues relating to processing of identity information;
* The Privacy Officer shall be an expert in data protection and privacy legislations, regulations and best practices;
* The Privacy Officer shall advise the top management on the privacy obligations;
* The Privacy Officer shall advise on high-risk processing and the requirement of data privacy impact assessments;

trainings shall be documented for audit purposes;

* Aadhaar specific trainings to developers, systems admins and other users shall be provided to ensure they are aware of the obligations for their respective roles; Completion of such trainings shall be documented;
* Privacy officer shall be responsible to formally communicate this policy to all stakeholders and staff who need to comply with this policy; Any changes to the policy shall be communicated immediately;
* Privacy Officer shall facilitate formal Privacy performance reviews with the relevant stakeholders / Privacy Committee and suggest improvements. The reviews shall consider the results of various audits, privacy incidents, privacy initiatives, UIDAI requirements etc.

# Transfer of Identity information outside India is prohibited

* Identity information shall not be hosted or transferred outside the territory of India in compliance to the Aadhaar Act and its Regulations.

# Grievance Redressal Mechanism

* Aadhaar number holders with grievances about the processing can contact the organisation’s Privacy Officer via multiple channels like on the website, through phone, SMS, mobile application etc.
* Reasonable measures shall be taken to inform the residents / customers / individuals about the Privacy Officer and its contact details;
* Following relevant documents shall be referred to for ensuring compliance to the Aadhar requirements:
  + Judgement of Honorable Supreme court dated September 2018
  + Aadhaar Act 2016
  + Aadhaar and Other Laws (Amendment) Act 2019
  + Aadhaar (Authentication) Regulations 2016
  + Aadhaar (Data Security) Regulations 2016
  + Aadhaar (Sharing of Information) Regulations 2016
  + Any other Regulations or notices or Circulars issued by UIDAI from time to time

# Contact Details

* + Name of Privacy Officer:
  + Phone:
  + [Email:](file://localhost/C:/Users/49327/AppData/Local/Microsoft/h)

|  |  |  |
| --- | --- | --- |
| 7 | CN | Common Name |
| 8 | Asset | An asset is anything that has value to the organization. Assets canbe classified into the following 5 categories:   * Paper assets: (Legal documentation, manuals, policies & procedures, organizational documents etc.) * Physical assets: (computer equipment, communications, utility equipment, buildings etc.) * Software assets: (database information, applications, software code, development tools, operational softwareetc.) * People assets: UIDAI human resources and stakeholders. * Service assets: (Logistics, building management systems, communications, utilities etc.) |
| 9 | Information/ Information Asset (IA) | Information that has value to the organization (UIDAI). Including butnot 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 |

importance. AUA shall ensure the confidentiality, integrity, and availability of these always by deploying suitable controls commensurate with the asset value and in accordance with applicable rules.

## Policy Scope

This Aadhaar Information Security Policy is applicable wherever UIDAI information is processed and/or stored by AUA . The policy may be amended from time to time as per regulations of UIDAI.2

Information Security Domains and related Controls

## Human Resources

* AUA shall appoint a SPOC/team for Aadhaar related activities and communication with UIDAI;
* AUA 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 thisinformation.
* Induction as well as periodic functional and information security trainings shall be conducted for all AUA personnel for Aadhaar related authentication services. The training shall include all relevantsecurity guidelines per the UIDAI information security policy for Authentication, Aadhaar Act, 2016 and Aadhaar Regulations, 2016.
  + All employees accessing UIDAI Information Assets shall be made aware of UIDAI information securitypolicy and controls.

application, audit logs, authentication servers, application, source code, information security

infrastructure etc.) processing UIDAI information;

* AUA employees with access to UIDAI information assetsshall:
* Have least privilege access for information access and processing;
* The operator must be logged out after the session isfinished.
* Implement an equipment locking mechanism for workstation, servers and/ or network device
* The application should have an 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.
* Access rights and privileges to information processing facilities for UIDAI information shall be revokedwithin 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
* 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;
* Common user IDs / group user IDs shall not be used. Exceptions/ risk acceptance shall be approvedand documented where there is no alternative;
* Procedures shall be put in place for secure storage and management of administrative passwords forcritical information systems. If done manually, then a fireproof safe or similar password vault must beused to

The access rules of firewalls shall be maintained only by users responsible for firewall administration.

## Password Policy

* The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first login;
* All User passwords (including administrator passwords) shall remain confidential and shall not be shared, posted, or otherwise divulged in anymanner;
* Keeping a paper record of passwords shall be avoided, unless this can be stored securely;
* If the passwords are being stored in the database or any other form, they should be stored in encrypted form.
* Passwords shall be changed whenever there is any indication of possible system or password compromise;
* Complex passwords shall be selected.
* Passwords shall not be hardcoded in codes, login scripts, any executable program or files;
* Password should not be stored or transmitted in applications in clear text or in any reversible form.
* Passwords shall not be included in any automated log-on process, e.g. stored in a macro or functionkey;

## Cryptography

* The Personal Identity data (PID) block comprising of the resident’s demographic ~~/~~ /biometric data shallbe
* The Common Name (CN) on the certificate presented by the AAS matches with its fully qualified

domain name (presently, auth.uidai.gov.in);

* Keymanagement activities shall be performed by AUA to protect the keys throughout their lifecycle.The activities shall address the following aspects of key management, including;
* key generation;
* keydistribution;
* Secure key storage;
* key custodians and requirements for dual Control;
* prevention of unauthorized substitution of keys;
* Replacement of known or suspected compromised keys;
* Key revocation and logging and auditing of key management related activities.

## Operations Security

* AUA shall complete the AADHAAR AUA on-boarding process before the commencement of formal operations;
* 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

computer code designed to damage or otherwise hinder the performance of, or access to, any PID information.

* 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 installedon such hosts.
* AUA shall ensure that the event logs are to be recorded and stored to assist in future investigationsand access control monitoring.
* 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;
* The authentication audit logs should contain, but not limited to, the following transactional details:
* Aadhaar Number against which authentication issought;
* Specified parameters of authentication request submitted;
* Specified parameters received as authentication response;
* The record of disclosure of information to the Aadhaar number holder at the time of authentication
* Record of the consent of Aadhaar number holder for theresident
* Details of the authentication transaction such as APIName, AUA / KUA Code, Sub-AUA,

and shall not be used for any otheractivities.

## Communications security

* 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 biometricreader and the device performing the encryption shall be secured against all security threats / attacks
* Terminal devices shall provide different logins for operators. These users shall be authenticated usingsome additional authentication scheme such as passwords, AADHAAR authentication, etc.;
* Each terminal shall have a unique terminal ID. This number must be transmitted with each transactionalong with UIDAI assigned institution code for the AUA as specified by the latest UIDAI API documents
* A Unique Transaction Number (unique for that terminal) shall be generated automatically by the terminal which should be incremented for each transaction processed;
* The network between AUA ASA shall be secured. AUA shall connect with ASAs through leased linesor similar secure private lines. If a public network is used, a secure channel such as SSL or VPN shallbe used.
* The AUA server shall be hosted behind a firewall. The firewall rules shall block incoming access requests to the AUA server from all sources;
* 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
* any other information that is linked or linkable to an individual

Examples included but not limited to: Name, Address, Date of birth etc.

rules.

Third Party

All external parties, including contractors/vendors, state and central government agencies and other statutory authorities – who have access

to MAFIL information assets or information systems.

|  |  |
| --- | --- |
| Data protection and security | Anyone collecting personal and customer information must fairly and lawfully process it, process it only for limited, specifically stated purposes, use the information in a way that is adequate, relevant and not excessive, use the information accurately, keep the information on file no longer than absolutely necessary, process the information in accordance with your legal rights, keep the information secure and never transfer the information outside the country without adequate  protection. |