General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000

1. Objective

The objective of this document is to assist the various government departments that collect, receive, possess, store, deal or handle (jointly referred to as "handle" or "handled" or "handling" in this document) personal information including sensitive personal information or identity information to implement the reasonable security practices and procedures and other security and privacy obligations under the IT Act 2000, section 43A (Information Technology rules, 2011 - Reasonable Security practices and procedures and sensitive personal data or information) and Aadhaar Act 2016.

2. Definitions

For the purpose of this document, the definitions as given in the IT Act 2000 and Aadhaar Act 2016 have been used. These are provided here for sake of clarity.

i. ***Personal information*** *means any information that relates to a natural person, which either directly or indirectly in combination with other information available or likely to be available with a body corporate, is capable of identifying such person*.

ii. ***Sensitive personal data or information*** *means such personal information which consists of information relating to:*

- *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*

iii. ***Identity information*** *in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information; wherein* ***biometric information*** *means photograph, finger print, Iris scan, or such other biological attributes of an individual*; and ***demographic information*** *includes information relating to the name, date of birth, address and other relevant information of an individual*.

3. Document structure

This document is structured to provide general guidelines to various Government departments that are handling Personal information or sensitive personal data or information as per the IT Act 2000, section 43 A and Aadhaar Act 2016.

4. Intended audience

The intended audience for this document from the various government departments that are handling personal information or sensitive personal data or information or identity information as defined above are provided as follows:

i. Information Technology department or division or function
ii. Technology department or division or function
iii. Legal department or division or function
iv. Information security department or division or function
v. Chief Information Security officer
vi. Chief Technology officer
vii. Chief Information Technology officer

5.0 Basic Actions Departments should undertake should include:

5.1 Organisation Structure, Awareness and Training

i. Identify and deploy an officer responsible for security in your organization/ department
ii. An individual in the organization must be made responsible for protecting Aadhaar linked personal data. That person should be in charge of the security of system, access control, audit, etc.
iii. Ensure all officials involved in any IT related projects read Aadhaar Act, 2016 and IT Act 2000 along with its Regulations carefully and ensure compliance of all the provisions of the said Acts.
iv. Ensure that everyone including third parties involved in Digital initiatives is well conversant with provisions of IT Act 2000 and Aadhaar Act, 2016 along with its Regulations as well as processes, policies specifications, guidelines, circular etc issued by the authorities from time to time.
v. Create internal awareness about consequences of breaches of data as per IT Act 2000 and Aadhaar Act, 2016.
vi. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

5.2 Technical and Process Controls

i. Follow the information security guidelines of MeitY and UIDAI as released from time to time.
ii. Informed consent – Ensure that the end users should clearly be made aware of the usage, the data being collected, and its usage. The user's positive consent should be taken either on paper or electronically.
iii. Ensure that any personal sensitive information such as Aadhaar Number, Bank Account details, Fund transfer details, Gender, Religion, Caste or health information display is controlled and only displayed to the data owner or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
iv. Verify that all data capture point and information dissemination points (website, report etc) should comply with IT Act and UIDAI's security requirements.

v. If agency is storing Aadhaar number or Sensitive personal information in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using Hardware Security Modules (HSMs). If simple spreadsheets are used, it must be password protected and securely stored.

vi. Access controls to data must be in place to make sure sensitive personal information including Aadhaar number and demographic data is protected.

vii. For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number based index.

viii. Regular audit must be conducted to ensure the effectiveness of data protection in place.

ix. Identify and prevent any potential data breach or publication of personal data.

x. Ensure swift action on any breach of personal data.

xi. Ensure that the system generates adequate audit logs to detect any breaches

xii. Ensure no sensitive personal data is displayed or disclosed to external agencies or unauthorized persons.

xiii. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure that all Aadhaar holders are able to use it effectively.

xiv. Multi-factor for high security - When doing high value transactions, multi-factor authentication must be considered.

xv. In case department is using Aadhaar Authentication, it should follow exception handling mechanism on following lines-

a. It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.

b. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.

c. If the schemes is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.

d. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.

xvi. All access to information, or authentication usage must follow with notifications/receipts of transactions.

xvii. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, SMS, physical-center, etc.).

xviii. Get all the applications that collect personal sensitive information audited for application controls and compliance to the said Acts & certified for its data security by appropriate authority such as CERT-IN empanelled auditors.

xix. Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

xx. Check all IT infrastructure and ensure that no information is displayed and in case it is displayed, please remove them immediately.

xxi. Ensure that adequate contractual protection is in place in case third parties are involved in managing application/ data centers

5.3 Data Retention and Removal

i. Ensure that the department has developed a data retention policy

ii. Ensure that you do not store personal sensitive information for a period more than what is required

iii. Delete/ remove/ purge the data after a specified period

5.4 Aadhaar Specific precautions

i. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc.

ii. Do not store biometric information of Aadhaar holders collected for authentication.

iii. Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.

iv. Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar

number if required to be printed, should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed

v. Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar Act. The purpose of use of Aadhaar information needs to be disclosed to the resident

vi. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.

vii. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room

viii. Do not permit any unauthorized people to access stored Aadhaar data

ix. Do not share Authentication license key with any other entity.

****