DO's and Dont's

Do's and Dont's for Aadhaar User Agencies/Departments

DO's:

1. Read Aadhaar Act, 2016 and its Regulations carefully and ensure compliance of all the provisions of the Aadhaar Act, 2016 and its Regulations.
2. Ensure that everyone involved in Aadhaar related work is well conversant with provisions of Aadhaar Act, 2017 and its Regulations as well as processes, policies specifications, guidelines, circular etc issued by UIDAI from time to time.
3. Create internal awareness about consequences of breaches of data as per Aadhaar Act, 2016.
4. Follow the information security guidelines of UIDAI as released from time to time.
5. Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
6. Verify that all data capture point and information dissemination points (website, report etc) should comply with UIDAI's security requirements.
7. If agency is storing Aadhaar number in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using HSMs. If simple spreadsheets are used, it must be password protected and securely stored.
8. Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.
9. For Aadhaar number look up in database, either encrypt the input andthen look up the record or use hashing to create Aadhaar number

based index.

10. Regular audit must be conducted to ensure Aadhaar number and linked data is protected.
11. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

12. 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.
13. Identify and prevent any potential data breach or publication of personal data.
14. Ensure swift action on any breach personal data.
15. Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.
16. Informed consent - Aadhaar holder should clearly be made aware of the usage, the data being collected, and its usage. Aadhaar holder consent should be taken either on paper or electronically.
17. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP, Face) to ensure all Aadhaar holders are able to use it effectively.
18. Multi-factor for high security - When doing high value transactions, multi-factor authentication must be considered.
19. Create Exception handling mechanism on following lines-
20. 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.
21. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.
22. 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.
23. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card orPIN or other means.
24. All authentication usage must follow with notifications/receipts of transactions.

25. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, sms, physical-center, etc.).
26. Get all the applications using Aadhaar audited & certified for its data security by appropriate authority such as STQC/CERT-IN.
27. Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

DONT's:

1. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.
2. Do not store biometric information of Aadhaar holders collected for authentication.
3. 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.
4. 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, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed.
5. 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.
6. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
7. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room
8. Do not permit any unauthorized people to access stored Aadhaar data
9. Do not share Authentication license key with any other entity.