(3)

KEONJHAR CENTRAL COOPERATIVE BANK LTD.

Estd - 1950
Reg. No - 69BL

KEONJHAR

Information Security Policy for Aadhaar Data

Of

Keonjhar Central Co-operative Bank Ltd.

1. Objective

The primary objective of this Information Security Policy is to ensure the protection, confidentiality, integrity, and availability of Aadhaar-related data as per the provisions of the **Aadhaar Act, 2016**, and associated regulations and guidelines. This policy sets forth the security measures that must be adhered to in order to safeguard Aadhaar data from unauthorized access, misuse, alteration, or loss while ensuring compliance with legal and regulatory requirements.

2. Scope

This policy applies to all employees, contractors, third-party service providers, and any other personnel who access or process Aadhaar data. It covers all forms of data storage, transmission, and processing within the organization, including cloud environments and physical data repositories.

3. Aadhaar Data Handling Principles

- **Collection**: Aadhaar data, including biometric and demographic information, must be collected only for legitimate purposes as defined by the Aadhaar Act and regulations.
- **Processing**: Processing of Aadhaar data must be done solely for the purpose for which it was collected and in accordance with the consent of the Aadhaar holder.
- **Storage**: Aadhaar data must be securely stored, encrypted, and accessible only to authorized personnel.
- **Transmission**: Data must be transmitted securely using encryption techniques to ensure confidentiality during transit.
- **Destruction**: Aadhaar data must be securely destroyed or anonymized when no longer required for processing or as mandated by the applicable law.

4. Security Requirements

- **Data Encryption**: All Aadhaar-related data, both at rest and in transit, must be encrypted using state-of-the-art encryption standards (e.g., AES-256).
- **Access Control**: Access to Aadhaar data should be based on the principle of "least privilege." Role-based access control (RBAC) and multi-factor authentication (MFA) must be implemented to restrict unauthorized access.
- **Data Integrity**: Measures such as hashing and digital signatures must be employed to ensure the integrity of Aadhaar data.
- **Audit Logging**: All access to Aadhaar data must be logged. Audit trails must be maintained for a minimum of 6 months to monitor for unauthorized access or manipulation of data.
- **Secure Applications**: Systems and applications processing Aadhaar data must undergo regular security assessments, including vulnerability scanning and penetration testing.
- **Incident Response**: A defined incident response protocol must be in place to immediately address any data breach or security incident related to Aadhaar data.

5. Compliance with the Aadhaar Act and Regulations

- **Aadhaar Act, 2016**: All handling of Aadhaar data must comply with the **Aadhaar Act, 2016**, and any amendments or regulations prescribed by the **Unique Identification Authority of India (UIDAI)**.
- **UIDAI Regulations and Guidelines**: The entity shall follow the security standards and requirements laid down by UIDAI, including those specified under **Aadhaar (Data Security) Regulations, 2016**.
- **Regulatory Audits**: The entity must submit to audits and inspections as required by UIDAI or any other regulatory authority and take corrective actions based on audit findings.

6. Roles and Responsibilities

- **Information Security Officer (ISO)**: The ISO will be responsible for implementing and enforcing this policy, coordinating security awareness programs, and ensuring compliance with security measures related to Aadhaar data.
- **Data Protection Officer (DPO)**: The DPO will monitor and ensure the protection of Aadhaar data and act as the point of contact for any data breach incidents.
- **Employees**: All employees must adhere to this policy and undergo regular security training related to Aadhaar data handling.

7. Security Awareness and Training

- Employees and contractors must undergo mandatory training on information security, with a special focus on handling Aadhaar data, data protection laws, and UIDAI guidelines.
- Periodic security awareness programs will be conducted to keep all relevant personnel up to date with security best practices and emerging threats.

8. Third-Party Access

- Third parties accessing or processing Aadhaar data must enter into a Data Protection Agreement (DPA) which will include specific security requirements, compliance with the Aadhaar Act, and incident response procedures.
- Regular audits and assessments will be carried out to ensure third-party service providers comply with security standards related to Aadhaar data.

9. Physical Security

- Aadhaar data must be stored in secure physical environments with access restricted to authorized personnel only.
- Security measures such as biometric access control, CCTV surveillance, and secure disposal of paper records containing Aadhaar information will be implemented.

10. Data Breach Management

- In the event of a data breach involving Aadhaar data, the entity must immediately inform UIDAI and affected individuals, if necessary, in accordance with the breach notification requirements.
- The entity must also carry out a root-cause analysis, mitigate the effects of the breach, and implement measures to prevent recurrence.

11. Continuous Improvement

- The entity will review and update this policy periodically to ensure its alignment with changes in the **Aadhaar Act**, regulatory updates, and emerging security threats.
- The effectiveness of the implemented security controls will be assessed regularly through internal audits and vulnerability assessments.

12. Enforcement and Consequences

- Non-compliance with this policy will lead to disciplinary actions, which may include termination of employment, contract termination, or legal actions depending on the severity of the violation.
- The entity reserves the right to take appropriate corrective and preventive actions to ensure compliance with this policy and applicable regulations.

13. Conclusion

The protection of Aadhaar data is of utmost importance. This Information Security Policy is designed to ensure that all employees, contractors, and third parties uphold the highest standards of security when handling Aadhaar data. The policy ensures compliance with legal obligations and establishes a robust framework for the secure processing of Aadhaar data.

This policy should be reviewed and updated regularly to address evolving security threats and ensure compliance with the latest legal and regulatory standards.