



The Balasore Bhadrak Central Co-operative Bank Ltd.
Head Office: O.T. Road, Balasore-756001

Aadhaar Security Policy for Balasore Bhadrak Central Co-operative Bank (BBCCB)

1. Purpose

This Aadhaar Security Policy provides comprehensive guidelines to safeguard the confidentiality, integrity, and availability of Aadhaar data managed by Balasore Bhadrak Central Co-operative Bank (BBCCB). The policy ensures compliance with the Aadhaar Act, ISO 27001:2022, NIST SP 800-53, UIDAI Security Guidelines (v4.0), and ISO 27701:2022 standards.

The policy is intended to define the approach BBCCB adopts to ensure that all Aadhaar data is collected, stored, processed, and transmitted securely, in full compliance with applicable legal, regulatory, and security standards.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and stakeholders who handle, access, or manage Aadhaar data within BBCCB. The scope includes all systems, processes, and infrastructure that collect, store, process, or transmit Aadhaar-related information.

3. Legal and Regulatory Compliance

BBCCB commits to adhere to the following:

- **Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (Aadhaar Act)**
- **UIDAI Security Guidelines (Version 4.0)**
- **ISO 27001:2022 (Information Security Management Systems)**
- **NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)**
- **ISO 27701:2022 (Privacy Information Management Systems)**
- **Other applicable national and international data protection laws**

This policy shall also ensure compliance with UIDAI regulations and other guidelines issued by regulatory bodies.

4. Policy Statements

4.1 Compliance with Aadhaar Act & UIDAI Regulations

- Aadhaar data shall only be used for **UIDAI-approved purposes** with explicit user consent.
- Biometric data **shall not be stored**; only use UIDAI-authenticated responses.
- Aadhaar numbers must be masked (e.g., XXX-XXX-1234) in displays/printouts.

4.2 Data Security Controls

- **Encryption:**
 - Aadhaar numbers stored only in **Aadhaar Data Vault** with AES-256 encryption.
 - Data transmission via TLS 1.2+ or VPN.
- **Access Control:**
 - Role-based access (RBAC) following the principle of least privilege.



The Balasore Bhadrak Central Co-operative Bank Ltd.

Head Office: O.T. Road, Balasore-756001

- Multi-factor authentication (MFA) for systems handling Aadhaar data.
- **Retention & Disposal:**
 - Retain Aadhaar data only as mandated by UIDAI; securely shred/destroy records post-use.

4.3 Incident Management

- Report breaches involving Aadhaar data to **UIDAI within 72 hours** via CERT-In.
- Conduct root-cause analysis and remediate gaps promptly.

4.4 Training & Awareness

- Annual training for employees on Aadhaar security, UIDAI guidelines, and phishing prevention.

4.5 Audits & Risk Assessments

- Conduct **bi-annual audits** aligned with ISO 27001 and NIST CSF.
- Perform risk assessments for Sub-AUA/Sub-KUA systems every 6 months.

4.6 Third-Party Management

- Ensure vendors comply with UIDAI's **Data Protection Policy** through binding agreements.

5. Roles and Responsibilities

- **Information Security Officer (ISO):** Responsible for overseeing Aadhaar security policy implementation, ensuring compliance with guidelines, and monitoring information security practices related to Aadhaar data.
- **Data Protection Officer (DPO):** Responsible for ensuring that all personal data, including Aadhaar information, is processed in accordance with the privacy laws and regulations.
- **Employees and Contractors:** All employees and contractors must follow the security procedures and policies outlined in this document and report any security incidents or breaches immediately.
- **Third-party Vendors:** Vendors who process Aadhaar data must comply with this policy and undergo security assessments to ensure they meet the required security standards.

6. Security Controls and Guidelines

BBCCB will implement a comprehensive security framework based on the following standards and guidelines:

6.1 Access Control (ISO 27001:2022, NIST SP 800-53)

- **Authentication:** Only authorized personnel will have access to Aadhaar data. Multi-factor authentication (MFA) will be required for all systems and applications that process Aadhaar data.
- **Role-Based Access:** Access to Aadhaar data will be granted on a need-to-know basis, following the principle of least privilege.
- **User Access Management:** Regular review of user access rights to Aadhaar systems will be conducted, and access will be revoked promptly when no longer required.

6.2 Data Encryption (ISO 27001:2022, NIST SP 800-53)



The Balasore Bhadrak Central Co-operative Bank Ltd.
Head Office: O.T. Road, Balasore-756001

- **Encryption of Aadhaar Data:** All Aadhaar data will be encrypted at rest and in transit using industry-standard encryption algorithms (e.g., AES-256) to protect it from unauthorized access or tampering.
- **Cryptographic Key Management:** Cryptographic keys used for encrypting Aadhaar data will be managed in compliance with NIST SP 800-53 control SC-13 to ensure the confidentiality and integrity of data.

6.3 Data Retention and Disposal (ISO 27001:2022, NIST SP 800-53)

- **Data Retention:** Aadhaar data will be stored only for as long as necessary for legitimate business purposes or as required by law.
- **Data Disposal:** When no longer required, Aadhaar data will be securely deleted or anonymized in compliance with ISO 27001 and UIDAI guidelines.

6.4 Incident Management (ISO 27001:2022, NIST SP 800-53)

- **Incident Reporting:** Any security incidents involving Aadhaar data must be reported immediately to the ISO and documented. An incident management process will be in place to respond promptly to any breaches.
- **Incident Response Plan:** BBCCB will maintain an **Incident Response Plan (IRP)** to manage and mitigate security breaches. The plan will include steps for containment, investigation, remediation, and communication to stakeholders and authorities, including UIDAI, as required by law.

6.5 Monitoring and Auditing (ISO 27001:2022, NIST SP 800-53)

- **Audit Logs:** All activities related to Aadhaar data access will be logged and stored for audit purposes. Logs will be regularly reviewed for signs of suspicious activity or unauthorized access.
- **Continuous Monitoring:** Systems that process Aadhaar data will be monitored in real-time for potential vulnerabilities or security threats. Security events will be analyzed and addressed promptly.

7. Third-party Management

BBCCB will ensure that third-party vendors who process Aadhaar data comply with this policy. The following measures will be taken:

- **Vendor Due Diligence:** Third-party vendors will undergo a thorough security assessment to ensure they meet the required standards for Aadhaar data protection.
- **Security Clauses in Contracts:** Contracts with third-party vendors will include clauses requiring compliance with this Aadhaar Security Policy, UIDAI guidelines, and applicable privacy laws.
- **Regular Audits:** BBCCB will conduct periodic audits to assess third-party compliance with security controls and identify any gaps in their data protection practices.

8. Training and Awareness

BBCCB will conduct regular security training for all employees to ensure they are aware of their responsibilities in safeguarding Aadhaar data, including:

- **Security Best Practices:** Training on data protection principles, secure handling of Aadhaar data, and how to recognize and report security incidents.



The Balasore Bhadrak Central Co-operative Bank Ltd.

Head Office: O.T. Road, Balasore-756001

- **Regulatory Compliance:** Educating employees on the Aadhaar Act, UIDAI guidelines, and other relevant regulations.
- **Security Awareness Campaigns:** Periodic campaigns to reinforce the importance of securing Aadhaar data and protecting individual privacy.

9. Privacy and Data Protection

BBCCB will implement controls to protect the privacy of Aadhaar holders, as prescribed under the ISO 27701:2022 for Privacy Information Management Systems (PIMS). These controls will ensure:

- **Consent Management:** Aadhaar data will only be collected and used with the explicit consent of individuals, as required by the Aadhaar Act and UIDAI guidelines.
- **Privacy Impact Assessments:** BBCCB will conduct regular privacy assessments to evaluate the impact of business processes or new systems on the privacy of Aadhaar data.

10. Review and Updates


This policy will be reviewed annually, or more frequently if necessary, to address changes in regulatory requirements, security best practices, and operational needs. The policy will be updated accordingly to ensure continued compliance with legal and security standards.

11. Conclusion

BBCCB is committed to securing Aadhaar data in line with the highest standards of information security, privacy, and legal compliance. By following the practices and guidelines outlined in this policy, BBCCB ensures the protection of Aadhaar data and maintains the trust of its stakeholders.

Approved By:


Chief Executive Officer


Chief Information
Security Officer (CISO)

References:

1. Aadhaar Act, 2016
2. UIDAI Security Guidelines (v4.0)
3. ISO 27001:2022 (Information Security Management Systems)
4. NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)
5. ISO 27701:2022 (Privacy Information Management Systems)