

# UIDAI DATA PROTECTION POLICY



## THE BHAWANIPATNA CENTRAL COOPERATIVE BANK LTD.

@Mahavirpada, Bhawanipatna, Odisha – 766001 📞 Tel: +916670–230786 / 230426 / 230380

✉ Email: [bccbho@bhawanipatnadccb.com](mailto:bccbho@bhawanipatnadccb.com) 🌐 Website: <https://bhawanipatnadccb.bank.in/>

**Document ID:** BCCB-IT-UIDAI\_DP/\_\_\_\_\_/2025

**Version:** 1.0

**Effective Date:**

**Prepared By:** Chief Information Security Officer

**Reviewed By:** Chief Executive Officer

**Approved By:** Board of Directors

**Classification:** Confidential - For Internal Use Only

# UIDAI DATA PROTECTION POLICY

(For AUA / KUA / Sub AUA / Sub KUA)

---

## 1. Purpose

The purpose of this policy is to establish a comprehensive framework for the protection, confidentiality, integrity, and lawful processing of Aadhaar data, personal data, and sensitive personal data handled by the AUA/KUA/Sub AUA/Sub KUA, in compliance with applicable laws, regulations, standards, and specifications issued by UIDAI and other statutory authorities.

---

## 2. Scope

This policy applies to:

- All Aadhaar Authentication and e-KYC related activities
  - All employees, contractual staff, consultants, and third parties handling Aadhaar data or personal data
  - All IT systems, applications, infrastructure, processes, and facilities used for data processing
  - All data in physical, electronic, or any other form
- 

## 3. Regulatory and Legal Framework

This policy is established in accordance with and shall be governed by:

### 3.1 Aadhaar Act and UIDAI Regulations

The organisation shall comply with:

- **The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016**
  - **All UIDAI regulations, circulars, guidelines, standards, and specifications** issued from time to time, including but not limited to:
    - Aadhaar (Authentication) Regulations
    - Aadhaar (Data Security) Regulations
    - Aadhaar (Enrolment and Update) Regulations
    - UIDAI Authentication & e-KYC API Specifications
    - Security and compliance advisories issued by UIDAI
-

### 3.2 Information Technology Act, 2000 (IT Act)

The organisation shall comply with the provisions of the **Information Technology Act, 2000** and amendments thereto, including:

- Protection of sensitive personal data and information
  - Implementation of reasonable security practices and procedures
  - Prevention of unauthorised access, damage, use, modification, disclosure, or impairment of data
  - Incident reporting and cyber security obligations
- 

### 3.3 SPDI Rules, 2011 and DPDP Act, 2023

#### a) Until DPDP Act comes into force

The organisation shall comply with the **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)**, including:

- Obtaining consent prior to collection of sensitive personal data
- Providing privacy notices to data subjects
- Ensuring secure storage, processing, and transmission of data
- Allowing review and correction of information
- Grievance redressal mechanism

#### b) On and from the date of coming into force of DPDP Act, 2023

The organisation shall comply with the **Digital Personal Data Protection Act, 2023** and all rules, notifications, and guidelines issued thereunder, including:

- Lawful, fair, and transparent processing of personal data
- Purpose limitation and data minimisation
- Accuracy and storage limitation
- Security safeguards for protection of personal data
- Rights of Data Principals
- Appointment and obligations of Data Protection Officer (where applicable)
- Data breach reporting and grievance handling

This policy shall be reviewed and updated to ensure alignment with DPDP Act requirements once fully notified.

---

## 4. Definitions

- **Aadhaar Data:** Demographic and biometric information collected under the Aadhaar Act.

- **Personal Data:** Any data about an individual who is identifiable.
  - **Sensitive Personal Data:** As defined under SPDI Rules / DPDP Act.
  - **Data Principal:** Individual to whom the personal data relates.
  - **Processing:** Any operation performed on personal data including collection, storage, use, disclosure, and deletion.
- 

## 5. Data Protection Principles

The organisation shall adhere to the following principles:

1. **Lawfulness, Fairness & Transparency** – Data shall be processed lawfully and transparently.
  2. **Purpose Limitation** – Data shall be collected for specified, explicit, and legitimate purposes only.
  3. **Data Minimisation** – Only necessary data shall be collected and processed.
  4. **Accuracy** – Data shall be kept accurate and up to date.
  5. **Storage Limitation** – Data shall be retained only as long as required.
  6. **Confidentiality & Integrity** – Data shall be protected against unauthorised access, alteration, or destruction.
  7. **Accountability** – The organisation shall be accountable for compliance with this policy.
- 

## 6. Lawful Collection and Consent

- Aadhaar and personal data shall be collected only for legitimate and authorised purposes.
  - Explicit consent shall be obtained from the Aadhaar number holder/Data Principal wherever required.
  - For minors, consent shall be obtained from parent/legal guardian.
  - Privacy notices shall be provided explaining purpose, usage, and rights.
- 

## 7. Data Usage and Disclosure

- Aadhaar data shall be used strictly in accordance with UIDAI guidelines.
  - Personal data shall not be disclosed to third parties except:
    - As required by law
    - With explicit consent of the data subject
    - As permitted by UIDAI / regulatory authorities
-

## 8. Data Retention and Destruction

- Data shall be retained only for the period required under law and UIDAI regulations.
  - Secure deletion / destruction mechanisms shall be implemented for data no longer required.
  - Retention schedules shall be documented and enforced.
- 

## 9. Security Safeguards

The organisation shall implement **administrative, technical, and physical controls** to protect data.

### 9.1 Administrative Controls

- Defined roles and responsibilities
- Background verification of personnel
- Confidentiality and non-disclosure agreements
- Periodic training and awareness programs
- Access approval and review mechanisms

### 9.2 Technical Controls

- Role-based access control (RBAC)
- Strong authentication mechanisms
- Encryption of data at rest and in transit
- Secure network architecture and firewall protection
- Anti-malware and endpoint security
- Logging, monitoring, and audit trails
- Regular Vulnerability Assessment & Penetration Testing (VAPT)

### 9.3 Physical Controls

- Restricted access to server rooms and work areas
  - CCTV surveillance and visitor controls
  - Secure storage of physical records
  - Environmental controls
- 

## 10. Rights of Aadhaar Holder / Data Principal

The organisation shall facilitate rights including:

- Right to information and access
- Right to correction and updating

- Right to withdraw consent (where applicable)
  - Right to grievance redressal
- 

### **11. Incident Management and Breach Reporting**

- A formal **Incident Response and Cyber Crisis Management Plan (CCMP)** shall be maintained.
  - All data breaches and security incidents shall be:
    - Detected and recorded
    - Investigated through root cause analysis
    - Reported to UIDAI, CERT-In, and other regulators as required
    - Remediated through corrective and preventive actions
- 

### **12. Audit and Compliance**

- Annual and need-based **Information Systems Audits** shall be conducted by a certified auditor.
  - Audit scope shall include compliance with:
    - UIDAI standards and Aadhaar (Data Security) Regulations
    - IT Act, SPDI Rules, DPDP Act requirements
  - Audit reports shall be documented and shared with UIDAI where required.
  - All non-compliances shall be tracked to closure.
- 

### **13. Third Party and Vendor Management**

- All service providers shall comply with UIDAI and data protection requirements.
  - Data protection clauses shall be included in contracts.
  - Periodic vendor assessments shall be conducted.
- 

### **14. Governance and Responsibility**

The **Aadhaar Nodal Officer / Compliance Officer / Data Protection Officer (as applicable)** shall be responsible for:

- Implementation of this policy
- Monitoring compliance
- Coordinating audits and regulatory communication
- Reporting to senior management

---

## 15. Training and Awareness

- Periodic training shall be provided to employees on:
  - Aadhaar data security
  - Privacy obligations
  - Incident reporting procedures
- Awareness communications shall be issued regularly.

---

## 16. Policy Review and Update

This policy shall be reviewed:

- At least **annually**, or
- Upon changes in UIDAI regulations, IT Act, SPDI Rules, or DPDP Act, or
- After major incidents or audit findings

---

## 17. Policy Publication

This Data Protection Policy shall be:

- **Published on the official website** [www.bhawanipatnadccb.bank.in](http://www.bhawanipatnadccb.bank.in)