DATA PROTECTION POLICY

Odisha e-Registration System

Aadhaar Authentication / e-KYC Environment

Version History

Version #	Prepared By	Revision Date	Approved By	Approval Date	Reason
1.0	Prasanta Kumar Samal	09/03/2025	Debarajan Mohanty	09/03/2025	Initial Version for e-KYC Audit

Table of Contents

Table of Contents

1. Purpose

This Data Protection Policy ("Policy") sets out the framework adopted by Terracis Technologies Ltd. ("the Entity"), acting as a Sub Authentication User Agency (Sub AUA) / Sub KYC User Agency (Sub KUA), for the protection of Aadhaar numbers, demographic information, biometric information, and other personal data collected, used, or processed in the course of undertaking Aadhaar-based authentication and e-KYC services. This Policy is issued pursuant to, and forms part of, the Entity's compliance obligations under the Aadhaar authentication ecosystem and applicable data protection law.

2. Scope and Applicability

This Policy applies to all employees, officers, contractors, vendors, and third parties of the Entity who collect, access, store, transmit, or otherwise process Aadhaar numbers or related personal data on behalf of the Entity, whether in physical or electronic form, across all systems, applications, and locations where such processing occurs.

3. Applicable Legal and Regulatory Framework

The Entity shall design, implement, and maintain data protection measures that are, at all times, consistent with the following laws, rules, regulations, and standards, as amended or superseded from time to time:

3.1 The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

The Entity shall comply with the Aadhaar Act, 2016, the Aadhaar (Authentication and Offline Verification) Regulations, 2021, the Aadhaar (Data Security) Regulations, 2016, and all other regulations, circulars, standards, and specifications issued by the Unique Identification Authority of India (UIDAI) from time to time, including but not limited to requirements relating to:

- Purpose and use limitation for Aadhaar numbers and authentication/e-KYC data;
- Consent-based collection and use of Aadhaar number and biometric/demographic information;
- Prohibition on storage of Aadhaar number, unless explicitly permitted, and mandatory storage in a separate, encrypted "Aadhaar Data Vault";
- Security safeguards for authentication infrastructure, including encryption, access controls, and audit logging;
- Restrictions on sharing and further disclosure of Aadhaar-related data; and
- Reporting obligations to UIDAI, including incident and breach reporting.

3.2 The Information Technology Act, 2000

The Entity shall comply with the Information Technology Act, 2000 ("IT Act"), including provisions relating to protection of data, reasonable security practices, and liability for negligent handling of sensitive personal data, as well as rules and notifications issued thereunder from time to time.

3.3 Transition from the SPDI Rules to the DPDP Act, 2023

The Entity recognizes the transitional data protection framework applicable in India and shall comply as follows:

- Until the Digital Personal Data Protection Act, 2023 ("DPDP Act") comes into force in full, the Entity shall comply with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules"), including requirements relating to a documented privacy/security policy, consent for collection of sensitive personal data or information, purpose limitation, and reasonable security practices such as an internationally accepted standard (e.g., ISO/IEC 27001).
- On and from the date on which the DPDP Act and the rules made thereunder come into force, the Entity shall comply with the DPDP Act and such rules, including (as applicable) requirements relating to notice and consent of Data Principals, purpose and storage limitation, data accuracy, reasonable security safeguards, breach notification to the Data Protection Board of India and affected Data Principals, and honoring of Data Principal rights (access, correction, erasure, grievance redressal, and nomination).

This Policy shall be read as automatically incorporating the DPDP Act and its rules upon their commencement, without requiring a formal amendment for this transition to take legal effect; a formal update to this Policy document shall nonetheless follow within a reasonable time to reflect the change.

4. Data Protection Principles

The Entity shall process Aadhaar numbers and other personal data in accordance with the following principles:

1. Lawfulness and Consent: Personal data shall be collected and processed only with the free, informed, specific, and unambiguous consent of the individual, and for lawful purposes connected with authentication or e-KYC services.
2. Purpose Limitation: Data shall be collected and used only for the specific purpose disclosed at the time of collection and shall not be used for any other purpose without fresh consent.
3. Data Minimization: Only such data as is necessary for authentication or e-KYC shall be collected.

4. Storage Limitation and Prohibition on Aadhaar Storage: The Aadhaar number shall not be stored except where explicitly permitted, and any permitted storage shall be in an encrypted Aadhaar Data Vault, segregated from other personal data.
5. Security Safeguards: Appropriate technical and organizational measures, including encryption, access control, network security, and logging/audit trails, shall be implemented to protect personal data against unauthorized access, use, disclosure, alteration, or destruction.
6. Accuracy: Reasonable steps shall be taken to ensure personal data processed is accurate, complete, and kept up to date.
7. Accountability and Grievance Redressal: The Entity shall designate responsible personnel, maintain records of processing, and provide a grievance redressal mechanism for data principals.
8. Breach Notification: Any data breach involving Aadhaar numbers or personal data shall be reported promptly to UIDAI and other competent authorities as required under applicable law, and to affected individuals where required.

5. Roles and Responsibilities

- Data Protection Officer / Nodal Officer: Responsible for overseeing implementation of this Policy, handling grievances, and serving as point of contact with UIDAI and regulators.
- Information Security Team: Responsible for implementing and monitoring technical safeguards, including the Aadhaar Data Vault, encryption, and access controls.
- Employees and Contractors: Responsible for complying with this Policy and reporting any suspected non-compliance or breach immediately.
- Senior Management / Board: Responsible for approving this Policy, allocating adequate resources, and reviewing compliance periodically.

6. Publication of this Policy

In accordance with applicable UIDAI requirements, this Policy shall be published in an easily accessible manner on the Entity's official website. The current URL at which this Policy is published is: **WWW.Igrodisha.gov.in/policy**Any change to this URL shall be updated in this document and communicated internally without delay.

7. Review and Amendment

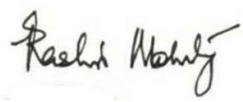
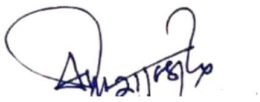
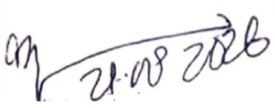
This Policy shall be reviewed at least annually, and additionally whenever there is a material change in the Aadhaar Act and regulations, UIDAI standards/specifications, the IT Act, the SPDI Rules, the DPDP Act and rules made thereunder, or the Entity's business

processes. All revisions shall be version-controlled and approved by Inspector General of Registration, Odisha prior to publication.

8. Consequences of Non-Compliance

Any violation of this Policy by an employee, contractor, or third party may result in disciplinary action, termination of contract, and/or reporting to competent authorities, in addition to any civil or criminal liability arising under the Aadhaar Act, the IT Act, the SPDI Rules, or the DPDP Act, as applicable.

9.Approval

Prepared By	Verified By	Reviewed By	Approved By
			
Prasanta Kumar Samal (TPOC)	Rashmi Mohanty (Project Head)	Sujay Kumar Pati (MPOC)	Mr. Deba Ranjan Mohanty (CISO)