

USE POLICY, CODE OF CONDUCT, SECURITY POLICY & RESTRICTIONS ON DESIGNING / COMPILING MALICIOUS CODE

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

1. Control Objective	3
2. Purpose	3
3. Scope	3
4. Applicable UIDAI and Regulatory Requirements	3
5. Key Prohibitions.....	3
6. Roles and Responsibilities.....	4
7. Policy Issuance and Acknowledgment Procedure (SOP)	4
8. Signed Staff Acknowledgment.....	5
9. Record Retention	5
10. Review and Amendment	5
11. Approval.....	6

1. Control Objective

Sub AUA / Sub KUA personnel should not intentionally write, generate, compile, copy, or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any Aadhaar information. This document sets out the Acceptable Use Policy, Code of Conduct, and security policy provisions adopted by Terracis Technologies Ltd. ("the Entity") to give effect to this control.

2. Purpose

The purpose of this document is to explicitly prohibit personnel of the Entity from writing, generating, compiling, copying, introducing, or attempting to introduce any malicious code — including but not limited to viruses, worms, trojans, logic bombs, ransomware, backdoors, or any other code designed to damage, disrupt, or hinder the performance of, or unauthorised access to, Aadhaar information or the systems that process it — and to ensure that this prohibition is formally acknowledged in writing by every relevant individual.

3. Scope

This document applies to all personnel of the Entity — including employees, contractors, interns, and any third-party/outsourced developers or support staff — who have access to, or the ability to write, modify, compile, or deploy code affecting, the Entity's Aadhaar authentication application, infrastructure, or Aadhaar-related information.

4. Applicable UIDAI and Regulatory Requirements

This restriction and the supporting policy framework shall be implemented in accordance with:

- UIDAI's Information Security Policy, the Aadhaar (Data Security) Regulations, 2016, and applicable circulars concerning malicious code and application security;
- The Aadhaar Act, 2016 and the Aadhaar (Authentication and Offline Verification) Regulations, 2021;
- The Information Technology Act, 2000, including provisions relating to computer contaminants, unauthorised access, and damage to computer systems;
- The Entity's Secure Software Development framework, Information Security Policy, and Change Logs Management procedure.

5. Key Prohibitions

- **No Malicious Code Creation:** Personnel shall not intentionally write, generate, compile, or copy any computer code designed to damage, disrupt, or degrade the performance of any system processing Aadhaar information, or to enable unauthorised access to Aadhaar information.
- **No Introduction of Malicious Code:** Personnel shall not introduce, or attempt to introduce, any such code into the Entity's Aadhaar authentication application, infrastructure, or any connected system, whether through direct code changes, scripts, macros, removable media, or any other means.
- **No Circumvention of Security Controls:** Personnel shall not write or use code intended to bypass, disable, or weaken access controls, encryption, audit logging, or other security controls protecting Aadhaar information.

- **No Unauthorised Testing:** Personnel shall not test, demonstrate, or experiment with malicious code techniques on the Entity's production or non-production Aadhaar authentication systems without explicit, documented authorisation (e.g., as part of an approved, contracted penetration test).
- **Mandatory Reporting:** Any personnel who becomes aware of malicious code, or a suspected attempt to introduce it, shall report the matter immediately in accordance with the Entity's Incident Management Procedure.
- **Acceptable Use:** Personnel shall use the Entity's systems and access strictly for authorised business purposes, and shall not use them to develop, test, store, or distribute malicious code for any purpose, whether related to the Entity's business or otherwise.

6. Roles and Responsibilities

- **All Personnel:** Comply with the Acceptable Use Policy, Code of Conduct, and this prohibition, and sign the acknowledgment required under Section 9.
- **Information Security Officer:** Owns and periodically updates the Acceptable Use Policy, Code of Conduct, and security policy provisions prohibiting malicious code; oversees detection and enforcement mechanisms (e.g., code review, SAST, endpoint protection).
- **HR Function:** Ensures the Acceptable Use Policy/Code of Conduct is issued to, and acknowledgment obtained from, every new employee at induction, and maintains signed acknowledgment records.
- **Engineering Lead / CTO:** Ensures code review and security testing practices (per the Entity's Secure Software Development framework) are capable of detecting any attempt to introduce malicious code.
- **Compliance Officer:** Maintains the approved policy documents and signed staff acknowledgments, and produces them for audit and UIDAI inspection upon request.

7. Policy Issuance and Acknowledgment Procedure (SOP)

The following procedure shall be followed to issue this prohibition and obtain evidence of acceptance:

- Step 1: Incorporate the prohibition on writing, generating, compiling, copying, or introducing malicious code into the Entity's Acceptable Use Policy, Code of Conduct, and/or security policy, as a standalone, explicit clause.
- Step 2: Issue the Acceptable Use Policy/Code of Conduct/security policy to every new employee, contractor, and relevant third-party/outsourced developer at induction, prior to granting access to the Aadhaar authentication application or infrastructure.
- Step 3: Obtain a signed acknowledgment from each individual confirming that they have read, understood, and agree to comply with the prohibition on malicious code, prior to or promptly upon commencement of access.
- Step 4: Re-issue the policy and obtain a fresh signed acknowledgment whenever the policy is materially revised, and periodically (at minimum, annually) as a refresher for all in-scope personnel.
- Step 5: Reinforce this prohibition through periodic training (see Training and Awareness / Secure Software Development documents) and internal communications.

- Step 6: Detect potential violations through code review, Static Application Security Testing (SAST), endpoint protection/anti-malware controls, and change-management review, in line with the Entity's Secure Software Development and Change Logs Management frameworks.
- Step 7: Investigate any suspected violation and take disciplinary and/or legal action as warranted, consistent with the Entity's Code of Conduct and applicable law, and document the outcome.
- Step 8: Retain the approved policy documents and all signed staff acknowledgments for audit and UIDAI inspection.

8. Signed Staff Acknowledgment

Each individual's acknowledgment of the prohibition on malicious code shall be recorded:

Tridib Pati	Assistant Manager	Tridib Pati
Sujit Kumar Singh	Assistant Manager	Sujit Kumar Singh
Sabyasachi Mohapatra	Assistant Manager	Sabyasachi Mohapatra
Asutosh Samal	Assistant Manager	Asutosh Samal
Manoj Kumar Muduli	Assistant Manager	Manoj Kumar Muduli
Siva Narayana Barik	Assistant Manager	Siva Narayana Barik
Amit Kumar Mohanty	Senior Software Developer	Amit Kumar Mohanty
Pravat Kumar Sahoo	Software Engineer	Pravat Kumar Sahoo
Sanjay Kumar Behera	Operator	Sanjay Kumar Behera
Abhas Kumar Dakua	Operator	Abhas Kumar Dakua
Akshya Kumar Sahoo	Operator	Akshya Kumar Sahoo
Chandrakata Penthoi	Operator	Chandrakata Penthoi

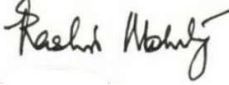
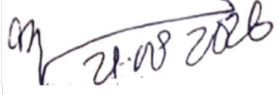
9. Record Retention

The Acceptable Use Policy, Code of Conduct, and security policy provisions prohibiting malicious code, together with all signed staff acknowledgments and the consolidated acknowledgment tracker, shall be retained in accordance with the Entity's record-retention policy and applicable regulatory requirements, and shall be made available to auditors and UIDAI upon request.

10. Review and Amendment

This document and the underlying policy provisions shall be reviewed at least annually, and additionally whenever UIDAI updates its Information Security Policy or issues relevant circulars, or upon any incident revealing a gap in this control. All revisions shall be version-controlled and approved by Inspector General of Registration, Odisha prior to circulation, and a fresh round of staff acknowledgment shall be obtained following any material revision.

11. 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)