

# BIOMETRIC DEVICE MANAGEMENT

## 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 |
|           |                      |               |                   |               |                 |

## Table of Contents

|                                                                   |   |
|-------------------------------------------------------------------|---|
| 1. Control Objective .....                                        | 3 |
| 2. Purpose.....                                                   | 3 |
| 3. Scope .....                                                    | 3 |
| 4. Applicable UIDAI Requirements.....                             | 3 |
| 5. Roles and Responsibilities .....                               | 4 |
| 6. Standard Operating Procedure (SOP) for Device Monitoring ..... | 4 |
| 7. Device Compliance-Monitoring Report.....                       | 5 |
| 8. Sample Review Sign-off.....                                    | 6 |
| 8. Compliance Summary.....                                        | 6 |
| 9. Record Retention.....                                          | 7 |
| 10. Review and Amendment.....                                     | 7 |
| 11.Approval.....                                                  | 7 |

## 1. Control Objective

Sub AUA / Sub KUA should monitor the operations of its biometric capture devices and related equipment periodically, for compliance with the terms and conditions, standards, directions and specifications issued and communicated by the Unique Identification Authority of India ("UIDAI") from time to time. This document sets out the policy and Standard Operating Procedure ("SOP") adopted by Terracis Technologies Ltd. ("the Entity") to give effect to this control.

## 2. Purpose

The purpose of this document is to ensure that all biometric devices (fingerprint scanners, iris scanners, and any other Registered Devices or Public Devices) and associated equipment used for Aadhaar authentication and e-KYC by the Entity, and by its authorized operators/agents, remain compliant with UIDAI-mandated device certification, registration, security, and operational requirements at all times, and that non-compliance is detected and remediated promptly through periodic monitoring.

## 3. Scope

This document applies to all biometric capture devices and equipment deployed by the Entity across its operator locations/branches, including devices used by Sub AUA/Sub KUA operators, franchisees, and other authorized points of authentication, and covers device onboarding, ongoing operational monitoring, and decommissioning.

## 4. Applicable UIDAI Requirements

Device operations shall be monitored for continued compliance with, including but not limited to:

- Use of only STQC/UIDAI-certified Registered Devices (RD Service compliant) as mandated by UIDAI;
- Valid and current device provider registration, device model certification, and RD Service application version;
- Device-level security features, including encryption of biometric data at the point of capture and secure key management;
- Device and RD Service auto-update compliance, including timely application of UIDAI-mandated patches and version upgrades;
- Operator authentication and biometric device binding requirements, where applicable;

- Prohibition on use of unregistered, tampered, cloned, or otherwise non-compliant devices; and
- Any additional terms, conditions, circulars, standards, or specifications issued by UIDAI from time to time.

## 5. Roles and Responsibilities

- Device Monitoring Owner: Responsible for maintaining the device inventory, scheduling periodic checks, and generating the compliance-monitoring dashboard/report.
- Information Security / IT Team: Responsible for verifying device certification status, RD Service versions, and security configuration.
- Field/Operations Team: Responsible for on-ground verification of devices at operator locations and escalation of non-compliant or suspect devices.
- Compliance Officer: Responsible for periodic sign-off on the monitoring report and escalation of unresolved non-compliance to senior management.

## 6. Standard Operating Procedure (SOP) for Device Monitoring

The following SOP shall be followed for periodic monitoring of biometric devices:

- Step 1: Maintain a live device inventory capturing device serial number, make/model, device provider, RD Service version, operator location, date of onboarding, and current certification status.
- Step 2: Conduct a compliance check of each active device at a defined frequency (at minimum, monthly, or as prescribed by internal policy/UIDAI direction), verifying device certification validity, RD Service version currency, and security configuration.
- Step 3: Cross-verify device certification status against the current UIDAI list of certified devices/providers and the latest UIDAI circulars and specifications.
- Step 4: Record the outcome of each check (compliant / non-compliant / requires update) in the device compliance-monitoring report or dashboard.
- Step 5: For devices identified as non-compliant, initiate remediation (e.g., firmware/RD Service update, device replacement, or deactivation) within a defined turnaround time and track closure.
- Step 6: Escalate unresolved non-compliance beyond the defined turnaround time to the Compliance Officer / senior management.



- Step 7: Perform a documented sample review of monitoring records on a periodic basis (e.g., quarterly) and obtain sign-off from an independent reviewer.
- Step 8: Retain all monitoring reports, dashboards, and sample review sign-off records for the period prescribed under applicable law/internal record-retention policy, and make them available for audit and UIDAI inspection upon request.

## 7. Device Compliance-Monitoring Report

A periodic device compliance-monitoring report shall be generated and maintained, at minimum capturing the following fields:

| Sl. No. | Compliance Check                        | Status   |
|---------|-----------------------------------------|----------|
| 1       | UIDAI Registered Device (RD) Certified  | Complied |
| 2       | RD Service Installed                    | Complied |
| 3       | Latest RD Service Version               | Complied |
| 4       | Device Firmware Updated                 | Complied |
| 5       | Device Driver Updated                   | Complied |
| 6       | Device Serial Number Verified           | Complied |
| 7       | Device mapped to Authorized Workstation | Complied |
| 8       | Antivirus Updated                       | Complied |
| 9       | Operating System Patched                | Complied |
| 10      | Device functioning properly             | Complied |
| 11      | Unauthorized Device Detection           | Nil      |
| 12      | Device Logs Available                   | Yes      |

The report shall be updated at each monitoring cycle and reviewed by the Device Monitoring Owner, with a summary shared with the Compliance Officer.



## 8. Sample Review Sign-off

On a periodic basis, a sample of monitored records shall be independently reviewed to verify the accuracy and completeness of the compliance-monitoring process. The sample review shall be documented and signed off as follows:

| Sl. No. | Review Item                       | Status | Remarks             |
|---------|-----------------------------------|--------|---------------------|
| 1       | UIDAI Registered Devices Verified | ✓      | Complied            |
| 2       | RD Service Installed              | ✓      | Complied            |
| 3       | Firmware Updated                  | ✓      | 3 devices scheduled |
| 4       | Drivers Updated                   | ✓      | Complied            |
| 5       | Unauthorized Devices              | ✓      | None                |
| 6       | Authentication Success Rate       | ✓      | Above 99%           |
| 7       | Device Inventory Verified         | ✓      | Matched             |
| 8       | USB Security                      | ✓      | Complied            |
| 9       | Incident Register Reviewed        | ✓      | No major incidents  |
| 10      | Preventive Maintenance Completed  | ✓      | Completed           |

## 8. Compliance Summary

| Item                           | Count |
|--------------------------------|-------|
| Total Offices Reviewed         | 321   |
| Total Devices Verified         | 321   |
| UIDAI Registered Devices       | 321   |
| Devices with Latest RD Service | 321   |
| Firmware Updated               | 318   |
| Firmware Pending Update        | 3     |
| Devices Replaced               | 2     |



| Item                  | Count |
|-----------------------|-------|
| Non-Compliant Devices | Nil   |
| Critical Issues       | Nil   |

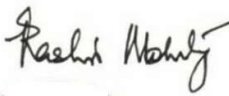
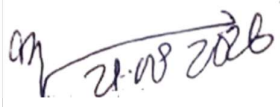
## 9. Record Retention

All device compliance-monitoring reports, SOP acknowledgements, and sample review sign-off records shall be retained in accordance with the Entity's record-retention policy and applicable UIDAI/regulatory requirements, and shall be made available to auditors and UIDAI upon request.

## 10. Review and Amendment

This document shall be reviewed at least annually, and additionally whenever UIDAI issues updated terms, conditions, standards, directions, or specifications affecting biometric devices. All revisions shall be version-controlled and approved by Inspector General of Registration, Odisha prior to circulation.

## 11. Approval

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