



Standard Operating Procedure (S.O.P)

Reporting mechanism by REs on the
Cyber-Incidents reported / identified pertaining to
Unauthorized Access to KYC Information on
CKYCRR

Document Control

Document Classification	Confidential				
Date	Version	Description of Change	Prepared by	Reviewed by	Approved by
19.11.2025	1.0	Initial Draft	ISD CERSAI	CISO	MD & CEO
28.04.2026	1.1	Modification in email ID for Incident Reporting by REs	ISD CERSAI	CISO	MD & CEO
27.08.2026	1.2	<p>Addition of the following aspects in SOP</p> <p>(a) Blocking the access of RE in cases of delay in reporting;</p> <p>(b) Carrying out Preliminary Investigation by the Central Registry based on incident reporting by RE and taking appropriate action.</p> <p>(c) Reporting the incident to CERT-In and Regulator(s);</p> <p>(d) Carrying out Root Cause Analysis, implement corrective actions, reporting action-taken report to CERT-In and Regulator(s) and formally closing the incident.</p>	ISD CERSAI	CISO	MD & CEO
27.10.2026	1.3	Addition of timelines for various tasks.	ISD CERSAI	CISO	MD & CEO

The Central KYC Records Registry (CKYCR) functions as a centralized repository for KYC records of customers in the financial sector, operating under the framework of the Prevention of Money Laundering Act (PMLA) and associated rules. In order to ensure data integrity, regulatory compliance, and to prevent unauthorized access to the CKYCR platform, it is crucial that only entities that are officially recognized and in good standing with their respective regulators are allowed access.

SOP: Reporting mechanism by REs on the cyber-incidents reported / identified pertaining to unauthorized access to KYC information on CKYCRR

1. PURPOSE & SCOPE

This SOP establishes a standardized reporting mechanism for REs to report cyber incidents involving unauthorized access to CKYCRR. This procedure applies to all REs utilizing CKYCRR services and covers incidents related to unauthorized access to CKYCRR. SOP also specifies actions to be taken up by CERSAI for investigating the incidents and reporting.

2. REPORTING REQUIREMENTS

REs must do Standard Reporting (Within 6 Hours) for following incidents related to unauthorized access to CKYCRR:

- a) Active data breaches or exfiltration
- b) Ransomware or malware infections
- c) Compromise of administrative credentials
- d) Unauthorized access to sensitive/regulated data
- e) Suspected unauthorized access attempts
- f) Failed authentication patterns exceeding thresholds
- g) Security control failures & Anomalous system behaviour
- h) Any other form of Cyber Attack

3. ACTIONS FOLLOWING THE INCIDENT

Step 1: Initial Detection & Assessment Reporting by RE (Within 6 Hours)

- a) Identify and verify the incident
- b) Assess severity and potential impact to CKYCRR
- c) Preserve evidence and logs
- d) Use prescribed reporting format (Annexure-1)
- e) Report to CERSAI by sending email to incident@cersai.org.in.
- f) Reporting to CERT-In and respective Regulator(s) of RE.
- g) Keep CERSAI, CERT-In and the Regulator(s) updated as the situation evolves, including any material developments, extension of impact, or change in severity of the incident.

Step 2: To be followed at CERSAI

- a) Carry out a preliminary investigation/assessment to ascertain the nature, scope and severity of the reported incident and its likely impact, if any, on the CKYCRR ecosystem.
- b) Suspend access to CKYCRR to the RE if deemed necessary to secure CKYCRR.
- c) Carryout reporting to RBI, CERT-In, NCIIPC.
- d) Perform thorough investigation of any traces of IoA/ IoC in CKYCRR systems and take remediation measures as necessary.
- e) Follow-up with the RE for further details on the incident.
- f) CERSAI shall initiate the above actions within six (6) working hours of receiving the intimation from the RE and shall perform the preliminary assessment within seven (7) working days. Wherever the assessment requires further inputs, CERSAI shall continue the assessment and may seek additional details from the RE, which the RE shall furnish within seven (7) working days.

4. ROLES & RESPONSIBILITIES

a) ROLES & RESPONSIBILITIES OF RE

- i. Timely incident detection and reporting
- ii. Evidence preservation and documentation
- iii. Coordination with internal teams
- iv. Implementation of containment measures
- v. Resource allocation for incident response

- vi. Decision-making authority for critical actions
- vii. Stakeholder communication
- viii. Reporting to CERT-In, Respective Regulators & CERSAI.

b) ROLES & RESPONSIBILITIES OF CERSAI

- i. Receipt, preliminary investigation and assessment of incident reports submitted by REs and taking appropriate action including temporary blocking/disconnection of the RE from the CKYCRR ecosystem where warranted.
- ii. Assessment of impact on CKYCRR systems managed by it and take necessary action as required to secure it.
- iii. Initial reporting to RBI, CERT-In and NCIIPC and subsequent updates.
- iv. Follow due diligence in restoration of RE access to the CKYCRR ecosystem upon satisfactory closure of the incident and confirmation of corrective action taken
- v. CERSAI shall initiate the above actions within six (6) working hours of receiving the intimation from the RE and shall perform the preliminary assessment within seven (7) working days. Wherever the assessment requires further inputs, CERSAI shall continue the assessment and may seek additional details from the RE, which the RE shall furnish within seven (7) working days.

5. Detailed Reporting, Root Cause Analysis & Closure of Incident by the RE

- a) Submit a comprehensive detailed incident report to CERT-In, the respective Regulator(s), and CERSAI
- b) Document the timeline of events
- c) Identify the systems and data affected
- d) Record the immediate action taken to contain the incident
- e) Participate in a Root Cause Analysis (RCA) to identify the underlying cause(s) of the incident
- f) Implement appropriate corrective and preventive measures to prevent recurrence
- g) Carry out Forensic Audit examination from CERT-IN empanelled auditor
- h) Take action on recommendations of auditor carrying out Forensic Audit.

- i) Carry out Cyber Security Audit from CERT-IN empanelled auditor of the RE infra facing CKYCRR with all observations closed & re-validated by the auditor
- j) Submit a post-incident report to CERT-In, the respective Regulator(s), and CERSAI, covering the RCA findings and corrective actions implemented
- k) Attach any communication received from CERT-In/Regulator(s) confirming closure of the incident and approval for resumption of normal services
- l) Carrying out Root Cause Analysis, implement corrective actions, reporting action-taken report to CERT-In and Regulator(s) and formally closing the incident.
- m) Efforts must be undertaken by the RE to respond to queries / documentation as mentioned above to CERSAI within 7 working days however in case of any delay due to legitimate reasons such as auditor on-boarding etc. the RE's access to CKYCRR shall remain blocked.

6. Restoring of RE Access to CKYCRR

Access of the RE shall be restored only after the RE submits the requisite incident report along with a satisfactory justification for the delay (where applicable), and CERSAI is satisfied that restoring access does not pose a risk to the security and integrity of the CKYCRR ecosystem. Prior to restoration of access, the RE shall be required to:

- a) Integrate with the CKYCRR testbed again and demonstrate their integration and the security measures implemented
- b) Carry out a Forensic Audit and submit the Forensic Audit Report from a CERT-In empanelled auditor
- c) Take action on the recommendations of the auditor carrying out the Forensic Audit
- d) Carry out a Cyber Security Audit from a CERT-In empanelled auditor of the RE's infrastructure facing CKYCRR, with all observations closed and re-validated by the auditor
- e) Submit a declaration-cum-undertaking, in the format prescribed by CERSAI, to CERSAI.
- f) Only upon satisfactory completion of the above, and CERSAI being satisfied that restored access does not pose a risk to the security and integrity of the CKYCRR ecosystem, shall access of the RE to CKYCRR be restored. The review of the RE's submission and the decision on restoration of access shall ordinarily be completed within seven (7) working days of receipt of the complete satisfactory submission

7. NON-COMPLIANCE

In the event an RE fails to report a cyber-incident pertaining to unauthorized access to CKYCRR within the prescribed timeline of six (6) hours from detection, CERSAI reserves the right to temporarily block/suspend the access of such RE to the CKYCRR ecosystem & reporting of the same to Regulator, without prejudice to any other action that may be initiated against the RE.