Incident Management Policy

The Sundargarh District Central Co-operative Bank Ltd.,

AT – REGENT MARKET, PO/DIST. – SUNDARGARH
PIN – 770001, ODISHA

Prepared on: 28th March, 2025

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★
Regd No.
90/56
1.6.1955

Ph: (06622) – 272022 ; 275050; 275022;
Fax : (06622) – 275122
E-mail:- sundargarhdccb@gmail.com

The Sundargarh District Central Co-operative Bank Ltd., SUNDARGARH – 770 001

Regd. No. 90/ SG / Dt.1.6.1955

Resolution by circulation of the Committee of Management of the Sundargarh District Central Co-Operative Bank Ltd., Sundargarh held on 28.03.2025

Agenda No. 01	**Resolution**
To consider to approve the updated Incident Management Policy of the Bank	The Committee of Management of the bank approved to updated Incident Management Policy with an addition of "Incident Reporting Procedure" (Point No. 8). The Chief Executive Officer is authorized to do the needful.

Copy to all members of the Managing Committee of Sundargarh District Central Co-Operative Bank Ltd., Sundargarh for confirmation.

Sd/-
Chief Executive Officer
Sundargarh DCC Bank Ltd., Sundargarh

Sd/-
PRESIDENT
Sundargarh DCC Bank Ltd., Sundargarh

//True Copy Attested//

Chief Executive Officer
Sundargarh DCC Bank Ltd., Sundargarh

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★
Regd No.
90/56
1.6.1955

Table of Contents

1. Introduction:

Incident Management is a process of IT Service Management (ITSM). This process is focused on returning the performance of the Bank's services to normal as quickly as possible with in Service Level Agreements (SLAs). Ideally, in a way that has little to no impact on Bank's core business and minimize impact on employee productivity from incidents. This policy helps IT teams to investigate, record and resolve service interruptions or outages.

The scope of incident management starts with an end user reporting an issue and ends with a service desk team member resolving that issue.

2. Roles & Responsibility of Incident Management Team/Managers:

i. Implementation of policy
ii. To inform users whom to report the incident
iii. Head of IT Department is expected to constitute CSIRT(Computer Security and incidence Response Team)
iv. Monitoring & Supervision of incidents
v. Set up process to meet business requirements
vi. Adhere to process and meet SLAs
vii. Manage teams at different levels and coordinate with other teams
viii. Generate reports and maintain Key Performance Indicators (KPIs)
ix. Be a point of escalation where a major incident needs to be resolved

3. Benefits of Incident Management:

- Better efficiency and productivity
- Visibility and transparency
- High level of service quality
- More insight into service quality by generating reports for visibility and analysis
- Better insight into Service Level Agreements whether or not they are met
- Prevention of incidents
- Improving mean time to resolution
- Reduction or elimination of downtime that occurs as a result of incident, which can slow or prevent businesses from executing operations and services
- Improving customer and employee experience

4. Computer Security Incident Response Team (CSIRT):

Bank should establish a CSIRT to handle reported incidents. The team consist of the following members:

a. Head of IT Department – DIT
b. External expert on Security incidents
c. Incident Manager - CISO
d. Security Manager
e. End Users

Charter of CSIRT – The CSIRT must have a charter which specifies what it should do, and the authority under which it will do it. The charter should include at least the following items:

i. Mission Statement
ii. Constituency
iii. Sponsorship/affiliation
iv. Authority

Functions of CSIRT:

CSIRT will assist system administrator/s in handling the technical and Bank's aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management.

a) **Incident Triage:**

- Investigating whether the extent an incident occurred.
- Determining the extent of the incident.

b) **Incident Coordination:**

- Determining the initial cause of the incident (vulnerability exploited)
- Facilitating contact with other similar sites who have reported the incident (if applicable)
- Facilitating contact with appropriate Law enforcement officials (i.e. The Government Cyber Security), if necessary
- Sharing reports to other CSIRT's
- Send out notifications to users, if applicable

c) **Incident Resolution:**

- Removing the vulnerability
- Securing the system from the effects of the incident
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or disciplinary action, if contemplated.

d) **Data Collection & Analysis:**

In addition, CSIRT will collect statistics concerning incidents which occur within or involve Bank's information resources and will notify the relevant parties proactively as necessary to assist it in protecting against known attacks.

e) **Incident Classification, Categorization & Prioritization:**

- The incident should be classified by the Incident Response Team (IRT) into the following categories:
  - i. Hardware
  - ii. Software
  - iii. Network
  - iv. Services
  - v. People
  - vi. Others
- Further sub-classification to the next level of granularity should be performed by the IRT.
- The incident must be categorized into security incident and/or major incident by the IRT.

f) **Policies for major incidents:**

- The following criteria can be considered while determine if an incident is a minor/major incident:
  - Functional Area criteria
  - Financial incident that could potentially lead to a loss
  - Service: 1- If there is downtime in service
2– If branch is down for more than one day
  - Site incident have affected more than one branch/site.
  - Service level incidents has affected critical service level targets that could result in financial penalty
  - Reputational incident may malign the brand image or popularity
  - Security incident have resulted or has highlighted a major security flaw or compromise
  - Health & Safety incidents has resulted in the deterioration of the health and safety of personnel, systems and/or infrastructure.
- Configuration items (CIs) affected by the incidents should be identified by the IRT. An impact analysis on the CIs affected by the incident should be performed by the IRT. This should identify the service(s) affected by the incident.

- Urgency of resolution of incidents should be determined on the basis of user input provided as part of the incident details or determining by the nature of incident and effected CIs. In case of difference between the two, the urgency should be determined by the nature of

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★ Regd No. 90/56 1.6.1955 incident.

- Depending on nature of incident, the incident should be assigned to the respective support groups by the IRT.

g) Incident Investigation & Diagnosis:

- The support Team (which may comprise of System Integrator's team and few members of IT division) should provide the initial support to resolve the incident to the satisfaction of the incident notifier based on results obtained by matching the reported incident to a known error/solution history/knowledge repository. Wherever possible, the incident notifier should be provided with means to continue the work interrupted by the incident, even if only with a degraded service.
- Each of the support team involved with incident handling should investigate and diagnose what has gone wrong. All investigation and diagnosis should be fully documented in the incident record so as to maintain the complete historical record of all incidents.

h) Incident Recovery:

- Once the potential resolution/work around has been identified, the same should be tested by the support team. Wherever possible/applicable, testing of the resolution/workaround should be performed in the test environment. The test environment should mirror the live environment as closely as possible. Even when the resolution has been found, sufficient testing should be performed to ensure that the recovery actions are complete.
- In case the incident is categorized as major incident, the categorization of the incident should be initially approved by the subject matter expert and by the incident Manager.

i) Incident Closure:

- It should be checked that the incident is fully resolved, and incident notifier is satisfied and willing to agree that the incident should be closed.
- While closing the incident record the following should be performed by the Incident Response Team (IRT):
    - ✓ Checking and confirming if the incident categorization/classification was correct. In case of incorrect categorization/classification, updating the records to reflect the correct data.
    - ✓ Obtaining a feedback from the incident notifier on the satisfaction of incident resolution.
    - ✓ Checking the completeness of the documentation associated with incident record
    - ✓ Deciding whether it is likely that the incident could reoccur and determining any preventive action to avoid this.

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★
Regd No.
90/56
1.6.1955

✓ Changing the status of incident to 'Resolved'.

- Once the incident notifier confirms the closure of incident, the incident status should be changed to 'Resolved' (or 'Technically closed'). Subsequently, after 48 hours the incident should be closed automatically, or the incident status changed to 'Closed'. The incident notifier has an option to foreclose or reopen the incident within 48 hours.
- The knowledge repository should be updated by the incident response team with any additional knowledge / know-how /learning / resolution/workaround/checklist/ initial support actions encountered during the course of incident lifecycle.
- The incident record should be periodically reviewed to ensure timely closure of incidents. Based on the review findings, escalations or corrective actions should be taken as required.

Note:

The following services to be provided by the Bank-

i. **Information Services:**
List of departmental security contacts, administrative and technical should be made available to all the users in the Bank and general public, via commonly available channels such as the Intranet/World Wide Web and/or the Domain Name Service.

ii. **Auditing Services:**
Central file integrity checking service to be done for various servers.

iii. **Archiving Services:**
Records of previous security incidents handled should be stored. While the records would remain confidential. Periodic statistical reports would be made available to the Bank's users.

5. Detection and initial reporting:

An incident may be detected by anybody in bank. The concerned personnel should immediately bring it to the notice of the person designated by CSIRT. The person so designated should escalate the issue as per escalation guidelines.

Incident reporting Form should contain at least the below mentioned details:

i. Department/Section:

ii. Date of reporting:

iii. Name of the employee reporting the incident:

iv. Designation of the employee reporting the incident:

v. Incident occurred date:

vi. Facts of the incident:

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. Regd No. 90/56 1.6.1955

vii. Analysis of the incident by Head of the Department/Section and its impact:

viii. Signature:

6. Documentation and formal reporting by CSIRT:

A person designated by CSIRT should maintain the central database of all such incidents. The person so designated, after analyzing the extent of expectation and facts of the incident, should appraise the CSIRT. A detailed risk and impact analysis for the incident should be carried out by the CSIRT. It should be the responsibility of the CSIRT to ensure that all incidents are categorized based on the nature of each incident and are held in a database created for the purpose. The database should be able to provide information on demand and have the capability to perform analysis on the data contained within.

SDCCB employees encountering incidents would thus be able to access the incident database and possibly find solution if the incident had occurred before. Frequently asked questions should also be incorporated into the database to assist the users in finding solutions to incidents encountered.

The Incident Management document should at least contain the following information and it should be filed /stored:

i. Incident Number:

ii. Incident Date:

iii. Branch/Department:

iv. Date of reporting:

v. Facts of the incident:

vi. Risk and impact analysis:

vii. Discussed with IT Committee on:

viii. Corrective action plan for incident management:

ix. Corrective action responsibility start date:

x. Date of completion:

xi. Expenditure incurred:

7. Monitoring:

All the major incidents should be reviewed and monitored by ITD every month and discussed in the IT Steering Committee meeting (IS Committee). The magnitude and criticality of the incidents may prompt designated ISM to discuss and take action on the incidents immediately instead of at fixed intervals.

8. Incident Reporting Procedure

This section provides detailed steps to report a security incident to the relevant authorities (UIDAI, RBI, NABARD, and CERT-IN) within defined timelines.

8.1 Initial Notification

- **Timeframe**: The incident must be reported within **2 hours** of detection.

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★
Regd No.
90/56
1.6.1955

- **Incident Detection**: Incidents may be detected through system alerts, user complaints, monitoring tools, or manual identification.
- **Action**: The Security Incident Response Team (SIRT) should immediately assess the incident and take the necessary actions for containment.

Initial Incident Report Template:

- **Incident ID**: [Unique Identifier]
- **Reported By**: [Employee Name/Role]
- **Date and Time of Incident Detection**: [DD/MM/YYYY, HH:MM:SS]
- **Nature of Incident**: [Data Breach, Malware Attack, Unauthorized Access, etc.]
- **Systems/Services Affected**: [List of affected systems/services]
- **Initial Containment Measures**: [Details of any immediate containment actions taken]

8.2 Reporting to UIDAI, RBI, NABARD, and CERT-IN

Upon detecting a security incident, a detailed incident report should be submitted to the relevant authorities based on the following guidelines:

- **UIDAI**: Any incident involving Aadhaar data (biometric or demographic) must be reported to UIDAI via the **UIDAI Data Security Incident Portal** or through official communication channels.
- **RBI/NABARD**: Incidents that affect banking operations or involve financial transactions must be reported to RBI or NABARD as soon as possible.
- **CERT-IN**: Any cybersecurity incident that could affect the national security framework or critical infrastructure should be reported to CERT-IN.

Reporting Timeline:

- **UIDAI**: **2 hours** (initial) and **24 hours** (detailed report)
- **RBI and NABARD**: **6 hours** (if applicable, related to financial transactions)
- **CERT-IN**: **6 hours** (if applicable, involving national security or critical systems)

Detailed Incident Report Submission:

- **Timeframe**: Within **24 hours** after initial detection.
- **Format**: The report must include the following details:
  - **Description of Incident**: Nature of the breach, how it was detected, and affected systems.
  - **Scope of Incident**: Specific data, users, and systems impacted.

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD.
Regd No. 90/56
1.6.1955

    - **Containment Actions Taken**: Immediate steps to contain the incident.
    - **Impact Analysis**: Preliminary impact on Aadhaar data and business operations.
    - **Preliminary Root Cause Analysis**: Initial findings on the cause of the incident.

8.3 Root Cause Analysis (RCA)

A detailed Root Cause Analysis (RCA) should be conducted to understand the underlying causes of the incident, assess its impact, and determine how the breach occurred. The RCA must be submitted to relevant authorities as part of the detailed incident report.

RCA Report must include:

- **Cause(s) of Incident**: System failure, human error, cyberattack, or external threats.
- **Incident Timeline**: Detailed account of the sequence of events from detection to resolution.
- **Analysis of Impact**: Data compromised, systems affected, and business disruptions.

8.4 Corrective and Preventive Measures

- **Corrective Measures**: Actions taken to immediately resolve the incident and minimize damage. For example:
    - **System Isolation**: Disconnect compromised systems to prevent further damage.
    - **Patch and Update**: Apply patches to vulnerable systems.
    - **Access Revocation**: Revoke compromised credentials or unauthorized access.
- **Preventive Measures**: Long-term steps to prevent recurrence, including:
    - **Enhanced Monitoring**: Implement more robust monitoring systems and intrusion detection systems (IDS).
    - **Employee Training**: Increase awareness and training programs on data security and incident response.
    - **Access Control Review**: Review and strengthen access control policies.
    - **Security Audits**: Conduct regular audits and penetration testing of systems.

8.5 Post-Incident Review

Once the incident is resolved, a post-incident review meeting should be conducted to:

- Evaluate the incident response process.
- Identify gaps in the incident management process.
- Ensure that corrective and preventive measures are implemented and effective.

The review meeting should involve key stakeholders such as the Information Security Officer (ISO), Data Protection Officer (DPO), legal, and compliance teams.

8.6 Continuous Improvement

After each incident, the Security Incident Response Plan should be updated based on lessons learned and areas for improvement. This includes revising procedures, adding new security controls, and conducting additional employee training.

---

9. Latest Incident Reporting Template

This template is used for reporting a security incident to UIDAI, RBI, NABARD, and CERT-IN. It ensures that the report is comprehensive and includes all relevant details.

Incident Reporting Template

Incident Report - [Organization Name]
Incident ID: [Unique Identifier]
Date of Detection: [DD/MM/YYYY]
Time of Detection: [HH:MM:SS]
Incident Type:

- Data Breach
- Unauthorized Access
- Malware Attack
- System Compromise
- Financial Fraud (for RBI/NABARD)
- Other: [Specify]

Incident Description:
[Detailed description of what happened, how the incident was detected, and the affected systems.]
Incident Impact:

- **Data Affected**: [Biometric data, demographic data, transaction data, etc.]
- **Number of Affected Users**: [Specify the number of Aadhaar users or customers affected]
- **Systems Affected**: [List of impacted systems or platforms]

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD.
Regd No.
90/56
1.6.1955

- **Business Impact**: [Description of business disruption, financial losses, or operational impact]

Initial Actions Taken:
[List of immediate actions taken to contain and mitigate the incident]
Root Cause Analysis (RCA):
[Explanation of the incident's root cause, including technical and organizational factors]
Corrective Measures:
[List of corrective measures taken immediately to resolve the incident]
Preventive Measures:
[List of actions to prevent similar incidents in the future]
Notification Details:

- **Reported to UIDAI**: [Yes/No, with timestamp of submission]
- **Reported to CERT-IN**: [Yes/No, with timestamp of submission]
- **Reported to RBI/NABARD**: [Yes/No, with timestamp of submission]
- **Contact Details**:
    - **Name**: [Incident Manager or Responsible Person]
    - **Role**: [Designation]
    - **Contact Information**: [Email, Phone]

Report Submitted By:

- **Name**: [Full Name]
- **Designation**: [Job Title]
- **Date and Time of Submission**: [DD/MM/YYYY, HH:MM:SS]

This template ensures that all security incidents are documented comprehensively and reported in a consistent and timely manner to relevant authorities.

10. Development of Corrective Action plan:

The CSIRT, in consultation with effected system administrator or any other person it deems fit should prepare the corrective action plan for the incident. The action plan, tough specific to each case, should typically cover the following:

a. Facts and explanation/reason for the incident
b. Corrective action to be taken
c. Estimated cost of implementing the corrective action
d. Estimated time frame, start date and end date
e. Personnel responsible for taking the action

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD.
Regd No.
90/56
1.6.1955

11. Confidential information Sharing:

The following information will not be released by CSIRT for general public:

a. Private user information about particular users, or in some cases, particular applications, which must be considered information for legal, contractual, and /or ethical reasons. However, if the identity of the user is disguised, then the information can be released freely (for example, to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).

b. Private site information of the technical nature except with permission of the site in question.

c. Vulnerability information without informing the relevant vendor a week in advance. However, if the vendor fails to respond in a week, Bank will be at its discretion to release the information at any forum it deems fit.

d. Any information that has been classified as confidential or restricted.

- **Escalation procedures:**

The central principles of escalation processes are-

a. All incidents for which this process is invoked will always be resolved at the lowest possible level of escalation.

b. Contact between provider organizations will always be between organizational peers. That is, the point of contact for a lower level of criticality will not directly contact the point of contact for a higher level of criticality within another provider's organization.

c. Expectations to the latter may not be made only by explicit mutual agreement on a per-incident basis.

Levels of Escalation:

a. Level one - Escalation level one is the initial level for all incidents. The contact must be available 24*365. The contacts at this level must have the ability to call IT official (IRT?) to take action and escalate to management as required, to resolve all categories and severity of incidents. This level consists of Helpdesk management executive or system administrators.

b. Level Two - Escalation Level Two represents the next level of management. Escalation to this level is appropriate only when Level One interaction has failed to result in resolution and further action transcends the authority of Level-One staff. This level consists of the Heads of IT Department of the Bank.

c. Level Three - Escalation Level Three represents senior management with authority to take actions that fall outside the standard operating policies of the concerned organizations. Escalation to Level Three is appropriate in cases where Level-One and Level-Two interactions have been unsuccessful in resolving an operational issue. This level consists of the management level employees.

Point of contact: Point-of-contact is required for each escalation level defined above. Telephone numbers and email addresses are required for each level.

- **Punitive Action for Violation:**

S. No	Description of Violation	High/Medium/Low
1	Failure to report an incident	
2	Failure to constitute CSIRT	
3	Non-adherence to the escalation procedure	
4	Improper management of incident, due to negligence or gross incompetence (such as failure to take corrective action within the necessary time)	
5	Failure by Third parties to give sufficient notice to Bank before initiating any change that could be described, or could lead to an incident	

*The action to be taken against the individual/group in violation of policy shall be decided by the IT Steering Committee (IS Committee) and as per Staff Service Regulations of the Bank depending on the severity and circumstances.

- **Review of the Policy:**

Taking into consideration of the circulars from RBI/NABARD, Chief Executive Officer is authorized to make suitable changes to the policy from time to time. Policy will be valid up to subsequent Board approval. Policy will be reviewed annually.

Chief Executive Officer

THE SUNDARGARH DISTRICT CENTRAL COOPERATIVE BANK LTD. ★
Regd No.
90/56
1.6.1955