Security Incident Management Policy and Procedure

Of

Keonjhar Central Co-operative Bank Ltd.

1. Objective

The objective of this Security Incident Management Policy is to establish a clear and structured procedure for handling security incidents that could impact the confidentiality, integrity, and availability of Aadhaar-related data, systems, and services. The policy includes guidelines for reporting incidents to relevant authorities such as UIDAI, RBI, NABARD, and CERT-IN, defined timelines for reporting, conducting Root Cause Analysis (RCA), taking corrective and preventive measures, and ensuring a continuous improvement process.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and external stakeholders who interact with systems or processes handling Aadhaar data. It covers the reporting, containment, resolution, and post-incident review for any security-related incidents affecting Aadhaar or related systems.

3. Definitions

- **Security Incident**: An event that compromises the confidentiality, integrity, or availability of information systems, leading to unauthorized access, data loss, or potential harm to systems or stakeholders.
- **Critical Incident**: A security incident that poses significant risks to the Aadhaar data or impacts business operations and requires immediate action and reporting to authorities.
- **Non-Critical Incident**: An event that is not immediately harmful but requires tracking and corrective measures to prevent future occurrences.

4. 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.

4.1 Initial Notification

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

4.2 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.
    - **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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

---

5. 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]
- **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.

---

6. Conclusion

The Security Incident Management Policy and Procedure outlined here ensures a systematic, efficient, and transparent approach to dealing with security incidents, particularly those related to Aadhaar data. By adhering to the defined timelines, conducting thorough investigations, and implementing corrective and preventive actions, the organization can significantly reduce the risk of data breaches and other security incidents.