THE OTTAPALAM CO-OPERATIVE
URBAN BANK LTD. No.F.1647

2024

Incident Reporting Policy

Incident Reporting Policy adopted by BOD vide resolution No.26(5)dt.02/12/2024

Version history	**1.0 Published on 02-12-2024**
Description of updates	**V1. Drafted and Reviewed** **V2. Reviewed**
Author	**System Administrator**
Reviewer	**Chief Compliance Officer**
Approved/Reviewed by	**Approved/ Reviewed by Board of Directors vide Resolution No.26(5) dt. 02-12-2024**

Table of content

1. Definitions

Ottapalam Cooperative Urban Bank means Its Head Office, branches and any other establishment or legal entity, including branches. Staff means all employees, workers, agency workers, consultants, directors, members and others.

- **Incident/Violation** - Any inappropriate activity, including financial crime, theft, fraud, harassment, affecting Ottapalam Cooperative Urban Banks interests or reputation, or any conduct relating to the discharge of professional duties by Staff.
- **Whistleblower** – a person who reports activity/persons believed to be or suspected of fraudulent or dishonest conduct
- **Retaliation** – Retaliation means any act of discrimination, revenge or harassment directly or indirectly taken against a whistleblower, by any person, for making a disclosure under the Policy.

- **Incident:** Any event that disrupts the normal operation of the Ottapalam Cooperative Urban Bank, poses a risk to security, compliance, or public safety, or could cause financial or reputational harm.

- **Critical Incident:** An event that causes significant operational disruption, financial loss, or could result in regulatory non-compliance or legal consequences.

- **Non-Critical Incident:** A less severe event that does not cause significant harm but requires attention to ensure it does not escalate.

The purpose of this policy is to outline the process for reporting incidents that may affect the Ottapalam Cooperative Urban Banks operations, security, regulatory compliance, or reputation. It ensures that all employees understand their responsibilities in identifying, documenting, and reporting incidents in a timely and accurate manner.

This policy envisages strengthening information security incident monitoring and management processes to include cybersecurity incidents and attempts in Ottapalam Cooperative Urban Bank.

Expected to report all unusual cyber security incidents (whether they were successful or were attempts which did not fructify) . Continuously update incident management policy and procedures to sanitize and share cyber security related incidents

2. Scope

This policy applies to all employees, contractors, and third-party vendors of the Ottapalam Cooperative Urban Bank. It covers all incidents, including but not limited to, any type of incidents - outage of IT, cybersecurity, theft or loss of information, outage of infrastructure, financial, cybersecurity breaches, fraud, compliance violations, system failures, operational disruptions, and any event that could affect the safety, security, and reputation of the Ottapalam Cooperative Urban Bank. Aim of this policy is to provide SECURE, VIGILANT and RESILIENT governance in Ottapalam CUB and their by provide seamless services to its customers .

3. Responsibilities:

1. **Employees:**

- All employees must immediately report any incidents they observe, suspect, or become aware of, regardless of severity.

2. Employees should document the incident details, including the time, nature of the incident, individuals involved, and any actions taken.

3. CBS provider – Since the bank is fully depending on the SaaS model services from the service provider, CBS provider should document the incident details, including the time, nature of the incident, individuals involved, and any actions taken with banks approval.

4. **Incident Reporting Officer (IRO)**

- The IRO will be responsible for overseeing the incident reporting process, ensuring timely response, and leading investigations.
- The IRO will maintain a log of reported incidents, classify them by severity, and ensure follow-up actions are completed.

4. Management:

- Branch Managers are responsible for ensuring their teams follow the reporting protocol and for assisting in the resolution of incidents when necessary.
- General manager is responsible for ensuring branches and head office follow the reporting protocol and for assisting in the resolution of incidents when necessary.
- MD/Management is required to report any serious incidents to the board team and regulatory bodies when appropriate.

5. Incident Reporting Procedure:

1. **Identification**
   - Employees should be vigilant in identifying any event or condition that could be categorized as an incident. Common incidents include system failures, suspicious financial transactions, security breaches, System Crash, Denial of service and regulatory violations.
2. **Immediate Action**
   - In case of an immediate threat to data security or physical safety, employees should act quickly to contain the incident (e.g., disconnecting compromised systems from banks network, alerting security personnel/branch manager).
3. **Reporting:**
   - Incidents should be reported through the designated incident reporting system (e.g., email, phone, or internal reporting software) immediately after identification.
   - The following details should be included (Not limited to)
     - Incident description

- Date and time of the incident
- Affected parties (internal and external)
- Immediate actions taken
- The current status of the incident

6. Incident Classification

The IRO or designated personnel will assess the reported incident and classify it as either critical or non-critical.

- **Critical Incidents** may require escalation to Chief information officer/Chief Security Officer, Senior management, regulators, or law enforcement.
- **Non-Critical Incidents** will be handled within the branch but must still be documented and tracked.

7.Investigation and Resolution

- Once an incident is reported, the CSO/IRO will lead an investigation to understand the cause, impact, and potential consequences of the incident.
- The investigation should identify corrective actions to prevent recurrence and document lessons learned.

8. Communication:

- Internal communication should be timely, ensuring that stakeholders, including management and affected departments, are aware of the incident and its impact.
- External communication with customers, regulatory authorities, or the media should be handled by the GM/Managing Director in coordination with chief Security/Information Officer, legal and compliance departments.

9. Follow-up and Documentation

- A post-incident review will be conducted to assess the response and identify areas for improvement with the help of Chief Information/Security Officer.
- All incidents must be logged in the incident management system, including a detailed report of actions taken, outcomes, and any follow-up required.

10. Confidentiality

All incident reports are confidential and should only be shared with authorized personnel involved in the investigation or resolution process. Employees must not disclose incident details to unauthorized parties.

11. Training and Awareness:

- All employees will undergo regular training on Cyber security, identifying and reporting incidents.
- The training program will cover security protocols, legal and regulatory requirements, and internal reporting procedures.

- Bank will send regular awareness SMS to its customers
- Bank will encourage whistle blowers

12. Policy Enforcement:

- Failure to report incidents in a timely manner or in accordance with this policy may result in disciplinary action.
- Employees found to have knowingly failed to report an incident or who have acted negligently in relation to incident management may be subject to face actions.

13. Review and Updates:

This policy will be reviewed annually or whenever there is a significant change to the Ottapalam Cooperative Urban Bank's operations, regulatory environment, or technological landscape. Any changes to the policy will be communicated to all employees.

14. Incident escalation matrix

1	Employee-Customer-Management: Problem reporting, initiating an incident	First level
2	Branch manager/IT Team	Initial investigation
3	CSO/IRO	Lead investigation against critical incidents
4	GM/MD/Board	External assistance/Reporting

15.Customers

To report any cyber incident, please email us at @ or call (ocubincident@gmail.com **& 046622443560 /9446235272)**

Cybercrime helpline number 1930.

For more information, please visit https://cybercrime.gov.in/.

,,,,,,,,,,,,,,,,,,,,,,,,,,,,

Annexure

(Attach latest incident format (if any) or use the same)

Sl No	Date	Problem description	Location	IP address of the suspected machine
			Branch Name	

Name & Signature of reporting officer

For investigation Officer -

Machine MAC Address:

Nature: Non-Critical/ Critical

Immediate Action -

Follow-up Investigation – Yes/No

Name & Signature of Investigating Officer

Board of Directors on 02-12-2024 vide Resolution No.26(5) approved the Policy on Incident Reporting .Board further resolved to designate Sri.Krishna Chandran T.M. ,Sr.Clerk as Incident Reporting Officer.

MANAGING DIRECTOR **DIRECTOR** **DIRECTOR** **CHAIRMAN**