Incident Management Policy

Version No: 1.0

THE JUTE CORPORATION OF INDIA LIMITED
PATSAN BHAWAN
ACTION AREA 1, CF BLOCK
NEW TOWN KOLKATA-700156

Effective Date: **12 /12/2024**

1. DOCUMENT DETAILS

Document:	Incident Management Policy
Document Number:	JCI/Policy/24-25/1
Version:	1.0
Document Date:	12.12.2024
Prepared By:	Prasenjit Saha, (Asstt. Mgr.-IT) (DISO) & A. Saha (CISO)
Reviewed By:	Avik Saha (Company Secretary)
Approved By:	Shashi Bhushan Singh(Managing Director),03.09.2025
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Date of Change	Version No.

Review History

Sl. No.	Reviewed by	Date of Review	Version No.

2. CONTENTS

3. OBJECTIVE

To ensure a robust incident management process to detect, report, respond and manage information security incidents.

4. SCOPE

Incident Management policy is applicable to all information assets. Further, this policy applies to all users such as employees, contractors and third parties accessing Organizations information assets.

5. STATEMENT

1. Incident Identification & Reporting

Sr No.	Policy Statements	Responsibility
1.	A formal process for Information security incident management shall be documented and implemented. It shall define the relevant roles and responsibilities associated with incident management.	IT Team
2.	A dedicated Incident Response Team (IRT) shall be formed to address the Information Security Incidents in an appropriate and timely manner. IRT shall consist of representatives from, IT, Admin and heads of other departments (based on applicability).	IT Team
3.	Organizations shall establish mechanisms to monitor Information Systems to identify and detect any anomalies. Detected anomalies shall be recorded and analyzed to check if they can be considered as Information security incidents.	IT team
4.	Information security incidents shall be identified from all relevant sources including users (employees, third parties, contractors), Security Operations Center, customers, threat advisories, etc.	IT Team IRT
5.	Organizations shall define and implement procedures for reporting incidents, violations and suspected security weaknesses. These procedures shall be communicated to all employees, contractors and third parties.	IT team

6.	All reported information security incidents shall be logged in a centralized system and classified based on their severity and impact to business.	IT team

2. Incident Response & Resolution

Sr No.	Policy Statements	Responsibility
1.	A root-cause analysis shall be carried out to understand the source of the incident and develop an appropriate plan for response and recovery.	IRT, IT Team
2.	Incident response plan shall be established and documented to ensure effective and timely resolution of the incident.	IRT, IT Team
3.	All evidences and audit trails related to incidents shall be collected and preserved in a secure manner to ensure authenticity, accuracy, completeness and chain of custody.	IT Team
4.	Organization shall involve forensic experts to perform forensic investigations for incidents requiring investigation for legal purposes/ critical information security incidents, if required.	CISO, IT Team
5.	Organization shall perform due diligence on technical sources, consultancy firms or forensic service firms before engaging for forensic investigation.	CISO, IT Team, Legal team
6.	Further to this policy, Incident Response & Forensics practices shall be followed as per organization Incident Response framework	IT Team
7.	Organization shall collect, process, store and analyze digital evidence in accordance with the regulations and laws that are applicable to organization environment in the relevant jurisdiction(s) for any security incidents where forensics evidence is required.	IT Team

3. Incident Escalation & Closure

Sr. No.	Policy Statements	Responsibility
1.	Organization shall define escalation matrix comprising of teams to be involved during various stages of information security incidents.	IT Team
2.	Information security incidents shall be tracked and communicated to affected stakeholders throughout the lifecycle of the incident	IRT, IT Team
3.	Incident closure shall be based on confirmation received from the affected party and verification of IT team.	Affected Party, IT Team

4. Contact with Authorities

Sr No.	Policy Statements	Responsibility
1.	Organization shall maintain appropriate contacts with the relevant authorities to inform and escalate incident to the respective authorities as required.	CISO, IRT, IT Team

5. Incident Repository & Review

Sr No.	Policy Statements	Responsibility
1.	Learnings from incidents shall be recorded and maintained to ensure that similar incidents are avoided in future.	IT Team IRT
2.	Organization shall perform periodic review of incident records including the identification of the incident trends, resolution effectiveness and deficiencies in incident resolution. The findings of the review shall be incorporated in the Incident Response plan to make it more effective.	IT Team, IRT

6. ENFORCEMENT

All users of organization who violate guidelines stated in this procedure may be subject to appropriate corrective action, including disciplinary measures.

7. REFERENCES

- ISO/IEC 27001:2022 Standard.