Incident Management Policy

Level 1 Policy

Document Information

Document Owner	IS Team
Document Approver	Board of Directors
Document Administrator	Mr. Arun Padmanabhan
Version	2.0
Effective Date	22-05-24
Distribution	All employees, contractors as per information classification and access policy With customers after approval from authorized personnel

Revision History

Date	Version	Changes	Made By	Reviewed By	Approved By
22-05-2024	1.0	Initial Version	IS Team	Arun Padmanabhan	Board of Directors
17-06-2025	2.0	No changes	IS Team	Arun Padmanabhan	Board of Directors

1. Summary

This Incident Management Policy outlines the requirements for managing Information Security Incidents and how these requirements apply to Edgro.

Edgro recognizes the need to follow established guidelines for addressing situations that could indicate compromise of Edgro information or disrupt Edgro business operations. Such guidelines include ensuring appropriate level of involvement of Edgro Management in the determination of actions to be implemented in response to an Information Security Incident.

2. Purpose

The purpose of this document is to ensure that Information Security Incidents are handled appropriately, effectively and in a manner, that minimizes adverse impact to Edgro.

3. Scope

This policy applies to all Edgro employees, third party contractors, consultants, temporary staff, vendors, and visitors. This Policy applies to Edgro's infrastructure, premises, all information, and information systems owned or administered by or on behalf of Edgro.

4. Roles and Responsibilities

Roles	Responsibilities	Authorities
CISO/IT Head	▪ Responsible for approving and reviewing the policy.	▪ Provide approval for incident management policy ▪ Review and approve the controls to be implemented for Incident Management
Incident Manager/IT Admin/IT team	▪ Driving the efficiency and effectiveness of the incident management process ▪ Producing Management information, including KPIs and reports ▪ Monitoring the effectiveness of incident management and making recommendations for improvement ▪ Ensuring that all the IT teams follow the incident management process for every incident	▪ Execute the incident response plan. ▪ Report to management about the status of incident management
IT Helpdesk	▪ Act as a point of contact for reporting information security incidents	▪ Provide resolutions and workarounds from standard operating procedures and existing known errors
Information security Team	▪ Responsible for the following: ▪ Monitor system for security breaches	▪ Evaluate and assign the incident severity

Roles	Responsibilities	Authorities
	▪ Document and catalogue security incidents ▪ Promote security awareness within the company to help prevent incidents from occurring in the organization	
Incident Response Team	▪ Incident Identification ▪ Incident assignment ▪ Functional escalation ▪ Investigation and diagnosis ▪ Incident review and closure	▪ Determine the appropriate course of action and the required resources needed
HR Department	▪ Responsible for communicating advisory to the employees involved in the repeat violations of higher severity.	▪ Authorized to take relevant disciplinary actions against employees and contractors
Employees	▪ Complying with this policy and with relevant legislation.	▪ Authorized to report incidents
Legal Team	▪ Responsible for providing necessary input for IT/Information security teams to interpret regulations.	▪ Authorized to report incidents

5. Policy

An information security incident is a single or a series of unwanted or unexpected information security events that has a significant probability of compromising business and threatening information security posture.

An information security incident includes, but not limited to, the following:

- Attempts (either failed or successful) to gain unauthorized access to data or information storage or a computer system.
- Unwanted disruption or denial of service to a system.
- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Unauthorized modification of data of information.
- Interference with the intended use or inappropriate or improper usage of information technology resources.
- Physical damage to an information asset.

5.1 Identification – Detection & Initial Reporting

- A security incident/security weakness can be detected by anybody in the organization and therefore authorizes anybody to report the incident to the appropriate functions.
- The incident can be reported verbally or through email to the Information Security Team. It shall be the responsibility of Information Security team to log and maintain all incident details in an appropriate system of record authorized by CISO/CTO.
- The Information Security incident shall be classified as IT security incident and non-IT incident.

IT Security Incident	Non-IT Security Incident
▪ Successful hacking attempt from the internet ▪ Web servers deface ▪ Virus and worm detection (unconfined); including advanced malware like Ransomware ▪ Unauthorized changes to the configuration of network and security devices ▪ Unauthorized modification of the webpages on the server ▪ Repeated active probes or port mapping from internet ▪ Attempted web page attacks or defacements launched from internet ▪ Application Server hacking attempt or phishing e-mails ▪ Virus or e-mail spam issues with multiple users ▪ Attempt to gain unauthorized access to the resources, either from within or outside the organization's network ▪ Unauthorized modification of production application system without prior approval	▪ Loss of VPN token ▪ Loss of customer provided assets ▪ Access card sharing ▪ Access control door not working ▪ Confidential documents lying unattended and in unlocked conditions ▪ Tailgating ▪ Infrastructure (CCTV, access controller, etc.) and network outages ▪ Physical damage

- The Information Security team and Incident Response team shall coordinate with respective functional heads for handling the incident based on the classification. Refer Annexure I for RACI matrix.
- Chief Technology Officer shall delegate the handling of the incident to Manager – IT/Admin & Infrastructure or managers of functions for further action. The manager shall collect the reported facts (symptoms of problem) of the reported incident and document these findings in an Incident report.
- The report shall at the minimum contain the following details, but not limited to:

1. Classification of incident (IT/ Non-IT)
2. Time of incident
3. Nature of incident
4. Detail facts of incident
5. Impact of the incident

- Following is an indicative list of all security incidents that should be reported:

1. Physical Security Incidents:
   - Fire/explosion/smoke
   - Electrical short circuit
   - Flood/water leakage/spillage of fuel
   - Damage to building structure
   - Physical harm to any employee/medical emergency
   - Electrical/mechanical breakdown (lift, generator), etc.
   - Intrusion by unauthorized people
   - Theft
   - Vandalism
   - Unidentified package lying unclaimed
   - Unlocked or unsecured access to critical storage room (server room)
2. Information Security Breach:
   - Server crash / loss of data or systems
   - Malware attacks - including viruses, worms, trojans, spyware, rootkits, etc.
   - ransomware attacks
   - Violation of information security policy, procedures or guidelines
   - Unauthorized access / modification / deletion of data
   - Theft or loss of Laptop / Media containing confidential data
   - Misuse of IT systems / computers
   - Misuse of Internet access / Email for accessing pornography, chain emails, defamation
   - Hacking into other systems internal or external
   - Cyber fraud - including phishing, spear phishing, vishing and whaling
   - Suspicious emails
   - Password sharing
   - Unauthorized use of other's user id or password
   - Confidential data / printed papers lying unclaimed or unsecured, etc.
3. Non-Adherence to Information Security Policies and Procedures:
   - Violation of company policies, like misuse of E-mail, Internet, USB, sharing password, sending internal documents to personal e-mail address, sending confidential / sensitive data to non-intended recipients, accessing sexually explicit sites, or continued repeated violation of company policies.
4. Others:
   - Fraud/misrepresentation/falsification of finance or accounting related information
   - Operational process related, salary or employee claims related etc
   - Physical damage to any assets including computers, electrical equipment etc

5.2 Incident Response Team

- The Incident Response team shall consist of the IT Head and program/functional heads to address any Information Security incidents and initiate immediate action to resolve the same.
- Incident Response Team shall be responsible for evaluating the incident and appropriately initiating the escalation process and holds the overall responsibility to monitor the activity and facilitate any action.

- Chief Technology Officer, IT Team and Information security team shall have the list of all emergency contact details of the entire Incident Response Team, vendors, suppliers, Service providers, etc.

5.3 Containment and Analysis

- The Incident Response team provides necessary inputs for preserving footprints (i.e., Digital/Physical). No modification should be done without knowledge of Incident Response team, to avoid risk of non-repudiation.
- The Incident Response Team analyses the evidence and if required, visits the location (place, computer, server, etc) to collect further details immediately and take appropriate steps to isolate and contain the incident if it can spread to other assets.
- If the team is unable to identify the probable cause and the probable resolution it should contact the vendors or any other appropriate personnel.
- In certain cases, an incident (e.g., internal fraud) needs to be reported to the law enforcement agencies. In such cases, evidence collection and investigation procedures shall be followed. Refer Annexure I for RACI matrix.
- In case the incident impacts Edgro's clients, Edgro's shall notify the client as recommended by their escalation procedures
- The IT Head shall form a special committee with law enforcement agencies to address the following:

    1. Establishing a prior liaison with law enforcement agencies
    2. Deciding when to involve these agencies
    3. Setting up means of reporting such crimes
    4. Establishing procedures for handling and processing reports of computer crime
    5. Planning for and conducting investigations
    6. Consulting the legal function and the Chief Technology Officer
    7. Involving senior management and the appropriate functions, such as legal, internal audit, and human resources
    8. Ensuring the proper collection of evidence, which includes identification and protection of the various storage media
- In special circumstances, the incident response team shall decide when and why an investigation should be conducted, and whether to involve law enforcement agencies. Privacy issues need to be considered prior to such investigations.

5.4 Evidence Management (Collection of evidence)

- The gathering, control, storage, and preservation of evidence are extremely critical in any legal investigation; since the evidence may be intangible and subject to easy modification without a trace so evidence must be carefully handled.
- Evidence shall be collected from the source carefully without changing the integrity of the incident and the evidence must be collected from the following:
    1. Telephone records
    2. CCTV tapes
    3. Audit trails
    4. System logs
    5. System backups
    6. Witnesses
    7. Emails, etc.

- The discovered evidence shall be recorded in a logbook mentioning - who found it, where it was found, when it was found. The evidence must be then tagged; due care shall be taken to protect the evidence from getting damaged.
- The evidence shall be stored in a location with restricted access. Access shall be enabled only to limited people include Chief Technology Officer, Incident response team.

5.5 Corrective Action and Recover

- The Incident Response team shall prepare the corrective action plan for the incident. The action plan, though specific to each case, should typically cover the following:
    1. Facts and explanation/reason for the incident
    2. Corrective action to be taken
    3. Estimated cost of implementing the corrective action (if applicable)
    4. Estimated time frame; start date and end date
    5. Personnel responsible for taking the action
- Based on the plan, the team shall act to correct and recover the systems. For Non – IT related incidents; Head – Admin & Infrastructure shall involve external agencies if required for recovery of affected systems / personnel.

5.6 Follow-up Action

- After each incident a lessons-learned exercise must be conducted by the Incident Response team and should be documented adequately.
- The Incident Response team shall identify the reasons for the occurrence of the incidents and actions to prevent such incidents from recurring; these actions shall be defined and implemented accordingly.

5.7 Periodic reporting and Trend analysis

To properly manage the stakeholder expectations, communication to all relevant stakeholders must happen at regular intervals. In the event of an incident with "High" severity, the important stakeholders (e.g., Line Reporting Managers, Business Unit Heads, Site Leads, Plant Heads, Country Managers, Infrastructure & Security Head, and CXOs etc.) must be communicated, if it is observed that the incident might have affected them in any manner.

Incident Response Team must ensure that incident details are provided to relevant stakeholders with updates on containment and recovery.

The IT Head shall review the incident log on a monthly basis. All incidents should be reported and discussed in the Information Security Committee meetings.

Following is an indicative list of parties to be informed in case of an Information Security incident is identified:

Type of incident	Report to
Physical Security Incident	▪ Immediate superior / Team Leader ▪ Security Guard ▪ Information Security Team ▪ Client (Need basis) ▪ Any Manager or admin and infrastructure personnel
Information security breach	▪ Immediate superior / Team Leader ▪ Information Security Team ▪ Client (Need basis) ▪ IT helpdesk

Other incidents	▪ Immediate superior / Team Leader ▪ Information Security Team ▪ HR Team ▪ Client (Need basis)

5.8 Learning from security incidents

Incident pattern, behaviour, similarities, and other trend information shall be discussed, and appropriate action initiated to prevent recurrences and to improve the overall security levels.

6. Governance

This policy shall be reviewed at least annually by the Chief Information Security Officer. Additional reviews may be triggered by major changes in corporate strategy, the regulatory environment and/or financial market conditions. Changes to the policy can only be made with the approval of the Senior Executive, Information Security Risk.

The Chief Information Security Officer is responsible for overseeing the implementation and management of the policy, in conjunction with the Compliance Department.

7. Policy and Procedure References

- Information Security Policy

8. Exceptions and Escalations

This policy applies to all departments unless an exception is formally requested and approved. Exceptions should be requested through the policy exception process and are subject to approval by Executive Management.

In the event an individual or department becomes aware of an exception, a request must be sent to and approved by Executive Management. In the event individuals become aware of non-compliance with this policy, they must notify Executive Management directly or report the concern to the Information Security Committee.

Non-compliance with this policy may incur disciplinary measures and consequences including progressive discipline up to and including termination of employment.

9. Annexure I – RACI Matrix

RACI	Description
R: Responsible	The executor(s) of the activity step
A: Accountable	The single owner who is accountable for the outcome of the activity
C: Consulted	The expert(s) providing information for the activity step
I: Informed	The stakeholder(s) who must be notified of the activity step

Process ID	Activities	Roles							
		End user/IT staff	Service Desk/IT Help Desk	Incident Response Team			Information Security Team	CTO	Legal Team
				Incident Manager	Incident Coordinator	Incident Analyst			
1	Incident Identification	R	R/A/I	R		R			
2	Incident logging	C/I	I	A			R		
3	Incident categorization	I	A/R	C/A	I	C	R	R	C
4	Incident prioritization	I	I	C/A		C	R		
5	Incident Assignment			A	R	R	C/I		
6	Functional Escalation			A/R		I	R		
7	Notify incident to clients			C/I			R	C	
8	Incident Investigation and Diagnosis	C/I		A	C/I	R	C/I	C	
9	Incident resolution and recovery	C/I		A	C/I	C	R		
10	Incident review	I	I	R	C/I	I	R	I	
11	Incident closure	I	I	R	C/I	I	R	I	
12	Report to the law enforcement agencies						R/I	R/I	C/I