Popular Vehicles & Services

Policy Related to Information Technology Security

INCIDENT MANAGEMENT POLICY

Document Title : Incident Management Policy

Version : 1.0

Effective Date : 31-01-2026

Review Cycle : Annual

Policy Owner : IT / Information Security

Approval Authority : Management / Board of Directors

1. Purpose

The purpose of this policy is to establish requirements for the identification, reporting, management, and resolution of information security incidents. This policy aims to minimize the impact of incidents on business operations, protect information assets, and support Information Security and Information Systems (IS) audit requirements.

2. Scope

This policy applies to all employees, contractors, consultants, and authorized third parties. It covers all information systems, applications, databases, infrastructure, and environments, including on-premises, cloud, and hybrid environments.

3. Incident Management Principles

The organization shall:

- Ensure prompt identification and reporting of incidents
- Respond to incidents in a timely and controlled manner
- Minimize the impact of incidents on business operations and information assets
- Maintain records of incidents to support analysis, remediation, and audit requirements

4. Definition of an Incident

An information security incident may include, but is not limited to:

- Unauthorized access or attempted access to systems or data

- Malware infections, ransomware, or cyberattacks

- Data loss, data leakage, or unauthorized disclosure

- System outages or failures impacting business operations

- Misuse of user accounts or security policy violations

---

5. Incident Reporting

- All suspected or confirmed incidents shall be reported immediately to IT / Information Security

- Incidents shall be reported through approved communication channels

- Users shall not attempt to investigate or resolve incidents independently unless authorized

---

6. Incident Response and Handling

- Reported incidents shall be logged, assessed, and categorized based on severity and impact

- Appropriate actions shall be taken to contain the incident, mitigate impact, and restore affected systems

- Incident response activities shall be coordinated by IT / Information Security

---

7. Incident Documentation and Tracking

- All incidents shall be documented, including description, date and time, affected systems, actions taken, and resolution status

- Incident records shall be retained for audit and compliance purposes

---

8. Roles and Responsibilities

IT / Information Security:

- Receive and assess reported incidents

- Coordinate incident response and remediation activities

- Maintain incident records and evidence

- Support audits and post-incident reviews

Management / System Owners:

- Support incident response and decision-making

- Approve corrective actions where required
- Ensure business impact is addressed

Users:

- Promptly report suspected or actual incidents
- Cooperate during incident investigation and resolution

---

9. Audit and Evidence

The following audit evidence shall be maintained and made available upon request:

- Incident register or incident tracking records
- Incident investigation and resolution documentation
- Evidence of corrective or preventive actions taken

---

10. Compliance

Compliance with this policy is mandatory. Non-compliance may result in disciplinary action in accordance with organizational policies and applicable laws. Approved exceptions shall be formally documented.

11. Review

This policy shall be reviewed annually, or earlier in the event of significant changes to systems, threat landscape, or regulatory requirements.

---

12. Approval

This policy has been reviewed and approved by the following authorities:

Role	**Name**	**Signature**	**Date**
Board of Directors/ Management			
Head – IT			