Incident Management Policy

Information Security

Version 1.0

Prepared By:
Hrushikesh Mehendale

Reviewed By:
Shruti Deshpande

FlaggGRC

Document Control

Last Modified	Reason For Change	Suggested By	Approved By
6 April 2025	Document created	Hrushi M	Shruti D
25 Mar 2026	Document reviewed, no change	Hrushi M	Shruti D
6 Oct 2026	Document reviewed, no change	Hrushi M	Shruti D

Purpose

This policy shall provide guidance on incident management.

Scope

All staff and third party users.

Principle

A process for reporting and management of information security incidents shall be established.

Reporting

The incident management process shall be defined including:

- Reporting
  - A process for reporting information security incidents shall be established and communicated to all the stakeholders.
- Verification
  - Reported incidents shall be verified and classified according to their security level.
- Oversight Committee
  - A committee shall be constituted to oversee the management of the reported incidents.
- Containment
  - Containment measures shall be put in place to mitigate the impact of the information security incident.
- External Notification
  - Criteria for notifying external authorities shall be determined.
  - The procedure for external authorities notification shall be established.
- Business Continuity
  - Criteria for invocation of business continuity protocol shall be defined.
  - Business continuity procedures shall be established.
- Analysis
  - Incident management shall include procedures for collection of evidence and analyzing the root courses.
- Recovery and Restoration
  - Systems shall be restored back to normal after the analysis.
- Learnings and Disciplinary actions
  - Policies and procedures shall be updated based on the learnings
  - Disciplinary actions shall be invoked if required

HaggGRC

⚙️Incident Management Procedure

Incidents

All information security incidents and their management activities shall be tracked in the incident and corrective actions register.

📓Incidents and Corrective Actions Register

Timelines

Response-times shall be defined for key steps in the incident management process.

- Verification of reported incidents
  - Within 4 business hours of reporting for non-complex scenarios
  - Within 8 business hours of reporting for complex scenarios
- Formation of oversight committee
  - Within 2 business hours of verification if all members are available
  - Within 6 business hours of verification in case members are not available
- Containment
  - Within 1 business day of committee formation for critical scenarios
  - Within 3 business days of committee formation for non-critical scenarios
- Business Continuity
  - Within 1 business day of committee formation for critical scenarios
  - Within 2 business day of committee formation for non-critical scenarios
- Analysis
  - Within 3 business days of committee formation for non-complex scenarios
  - Within 7 business days of committee formation for complex scenarios
- Recovery and Restoration
  - For critical scenarios
    - Within 5 business days of committee formation for critical path functionality
    - Within 10 business days of committee formation for entire functionality
  - For critical scenarios
    - Within 7 business days of committee formation for critical path functionality
    - Within 14 business days of committee formation for critical path functionality

FlaggRC

Monitoring

The incident management process shall be monitored on a bi-annual basis to ensure policy adherence.

📓 Incidents and Corrective Actions Register

Policy Compliance

Exceptions

Any exception to this policy shall be approved and recorded by the CISO in advance and reported to the Management Review Team.

Non-Compliance

Any staff found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

Continual Improvement

This policy is updated and reviewed as part of the continual improvement process.

FlaggGRC