Incident Management Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this policy is to provide a framework within which information security events and incidents associated with information systems are communicated in a timely manner and necessary corrective actions are taken.

2. Scope

This document is applicable to all processes and operations in CNTXT within the scope of the ISMS.

3. Policy Statement

Security incidents are irregular and anomalous conditions that cause — or may lead to — service degradation, loss of sensitive data, outages, or any form of reduced operational status. These situations require quick human intervention to avert disruptions or restore the operational status.

This document offers guidance and establishes methods for handling and managing incidents for the staff or incident responders who believe they have discovered or are responding to a security incident.

4. Information Security Incident Management

4.1 Responsibilities and Procedures

- An Incident management procedure shall be created to define procedures and responsibilities to ensure quick, effective, consistent, and orderly responses to information security incidents.
- There shall be responsible personnel appointed for:
    - Investigation/coordination of the reported information security incidents and security weaknesses.
    - Tracking closure of incidents and corrective and preventive actions.

4.2 Reporting Information Security Events and Incidents

- CNTXT's management shall establish appropriate channels through which information security incidents can be reported as quickly as possible.
- All information security incidents shall be recorded in an information security incident database.
- The details of the steps to be followed for reporting an incident shall be communicated to all employees and contractors of the company.
- Incident reporting and management procedures shall be made available for easy access and reference for reporting security incidents and weaknesses by the users.
- A monitoring mechanism shall be set up for proactive monitoring of intrusions, attacks, and frauds.

4.3 Assessment of and Response to Information Security Incidents

- All information security incidents that are reported shall be assessed and classified as per the classification criteria mentioned in the incident management procedure.
- The assessment and classification of incidents shall be maintained for future reference to allow easy identification and avoid false positives.
- A response plan and strategy for the appropriate handling of security incidents shall be formulated, which covers the incident cycle from identification to root cause analysis to resolution.
- The overall response to reported incidents shall include the identification of corrective action where important.
- Where a follow-up action against a person or organization after an Information Security Incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction.

4.4 Learnings from Security Incidents

- The analysis shall be carried out for the information security incidents and shared with the appropriate authorities periodically.
- Knowledge gained from the resolution of security events shall be used to reduce the likelihood of similar incidents in the future and help with limiting the impact of the incident.

5. Document security classification

Company Internal (please refer to the Data Classification policy for more details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Incident Management Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024