Incident Management Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this document is to establish a consistent and effective approach to the management of incidents throughout their lifecycle - from identification, assessment, corrective actions, and closure.

2. Scope

This document is applicable to all staff members at CNTXT performing various operations within the scope of the Information Security Management System (ISMS) (refer to the definition in Section 3 of the Information Security Policy).

3. Information Security Incident Management

3.1 Responsibilities

- An Infra Operations person shall be appointed for:
  - Investigation/coordination of the reported Information Security incidents and Security weaknesses.
  - Tracking closure of incidents and, if required, ensuring identified corrective and preventive actions are taken.
- It is the overall responsibility of the Infosec officer to ensure that any incidents are dealt with appropriately.

3.2. Reporting Information Security Events and Incidents

- Where feasible, monitoring mechanisms are set up in CNTXT for proactive monitoring of intrusions, attacks, and frauds.
- Incidents at CNTXT can be reported in two ways:
  - Automated Threat Detection Services Such as AWS Guard duty - Such services monitor the infrastructure account and workloads for potential threats to the network. It shall analyze all relevant logs, including but not limited to system, network, performance, and application logs. If any threats or anomalous are detected, the findings will automatically be reported as incidents into a company-managed portal where they are tracked for investigation.
  - Staff Reported incidents – If any incident or security weakness is observed by employees during the course of operations must be reported. This communication portal shall be made available to all employees at all times.
- In case any employee notices any malicious behavior by a CNTXT staff member or partner, they should inform this incident directly to the Information Security Officer or the CEO. In such cases, they are strongly recommended to not discuss the issue with any other employee.

- A log of all security incidents reported shall always be maintained.

3.3 Responding to Security Incidents

- At any given point in time, the On-Call-Engineer (OCE) is the first point of contact and is responsible for addressing the incident. Among other things, their responsibility to identify the severity of the incident as per the definitions below:
    - Low severity Incidents are those that do not require immediate remediation. These typically include a partial service of CNTXT being unavailable (for which workarounds exist). These do not require someone to be paged or woken up beyond normal work hours.
    - Medium severity incidents are similar to Low but could include scenarios like suspicious emails or unusual activity on a staff laptop. Again, these do not require immediate remediation or trigger automatic calls outside work hours. Low and medium-severity incidents usually cover the large majority of incidents found.
    - High-severity incidents are problems an active security attack has not yet happened but are likely. This includes situations like backdoors, malware, and malicious access to business data (e.g. passwords, payment information, vulnerability data, etc.). In such cases, the Information Security Officer and the Engineering team must be informed, and immediate remediation steps should begin.
    - Critical severity incidents are those where a security attack was successful and something important was lost (or irreparable damage caused to production services). Again, in such cases, immediate actions need to be taken to limit the damage.
- It is the responsibility of the On-Call engineer to notify the Infra Operations person, Information Security Officer, and any other relevant stakeholder immediately in case of any incidents that are classified as “High” or “Critical”.

3.4 Incident Response and Resolution

- Once an incident is reported, a staff member or team will be assigned by the Infra Operations person to handle the incident. It is the responsibility of this person or team to investigate the incident and decide the appropriate response to the incident.
- For all incidents where there was no data loss or direct impact on the availability of CNTXT’s services, the details of the investigation and corrective actions taken shall be documented as a part of incident closure notes.
- For critical issues, the response team will follow an iterative response process designed to investigate, contain the exploitation, remediate the vulnerability, and write post-mortem and lessons-learned documents. Further, the following steps will be taken for critical incidents:
    - The ISO/CEO will determine if a lawyer should be involved with attorney-client privilege.

- A staff member or team will be assigned to handle the incident. This person or team will be responsible for limiting the damage of the incident, bringing the system back to operational status, and updating the leadership on the status as required.
- The team should create a timeline of known data related to the incident. The timeline should detail what we know the attacker did and at what times.
- The team should also recommend long-term mitigations to suggest steps in order to avoid a similar crisis in the future.
- In case of security incidents of specific kinds (like loss of data or data theft), the company leadership shall take steps to communicate with affected customers.

3.5 Learning from Critical Incidents

- The analysis shall be carried out to determine the cause, effect, mitigation, and lessons learned for the Critical Information Security Incidents and shared with the management of CNTXT and appropriate authorities.
- Knowledge gained from the resolution of such incidents shall be documented and should be used to reduce the likelihood of similar incidents in the future and help with limiting the impact of the incident.
- The analysis should also consider, wherever possible, costs incurred due to information security incidents.
- The output of the analysis shall be used to improve the security posture and to identify recurrence or impact tolerance.

3.6 Collection of Evidence

- 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(s).
- Before the seriousness/criticality of the incident is realized, due care shall be taken to ensure that necessary evidence/information is not destroyed intentionally or accidentally.

3.7 Contact with Authorities and Special Interest Groups

- The Information Security Officer should maintain contact with external authorities, special interest groups, and forums (e.g., law enforcement, Cyber security team, customers) for information security incidents.
- As per the applicable regulatory directives, the Information Security Officer should maintain contact with appropriate government authorities and report any incidents observed promptly.
- Membership in special interest groups or forums should be considered as a means to:

- Improve knowledge about best practices and stay up-to-date with the relevant security information.
- Ensure the understanding of the information security environment is current and complete.
- Receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities.
- Gain access to specialist information security advice.
- Share and exchange information about new technologies, products, threats, or vulnerabilities.

4. Document Security Classification

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

5. 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.

6. 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.

7. Schedule

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

End of Incident Management Procedure. 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