ISMS Information Security Roles & Responsibilities

Version 1 - Approved by Youssef Ouyhya

Contents

1. Purpose

This procedure supports the high level policy statements defined in Information Security Policy. The purpose of this document is to detail the organization structure for information security in CNTXT FZCO (henceforth referred to as CNTXT or company or organization).

2. Organization of Information Security

2.1 Roles and Responsibilities

2.1.1 CEO

- Responsible for Information security policy and controls to assure compliance with applicable regulatory and legal requirements as well as good business practices;
- Provide business-level strategy inputs towards improvement of ISMS;
- Review the impact on organization of compliance changes;
- Build a security risk profile of the IT landscape in relation to the future business;
- Responsible for governing the implementation of new technologies in security to mitigate security threats or breaches;
- Adequate regulatory and budget to implement security roadmap;
- Approving major initiatives to enhance information security; and
- Providing adequate resources (financial, human) to implement and improve the ISMS at CNTXT.

Authority

- Has ultimate authority over all decisions regarding organizational changes
- To take financial decisions on issues related to risk.

Key Skills & Competencies

- Understand the business.
- Understand the business need for protection.
- Understand the business 'impact' of violation.
- Access to the ISMS roles & responsible documents.

2.1.2 Information Security Officer

Roles & Responsibilities:

- The Information Security Officer shall report to the CEO and have overall responsibility of establishing, implementing, operating, monitoring, reviewing, maintaining and improving the ISMS;
- The Information Security Officer shall review the ISMS policies, procedures, templates and other documentation;
- The Information Security Officer shall be the owner & custodian of the ISMS documentation;
- The Information Security Officer shall be responsible for coordinating the information security reviews yearly;
- Reviewing the Risk Assessment methodology, Risk Acceptance Criteria, Risk Assessment, residual risks, and risk mitigation action plans;
- Information Security Officer shall ensure the following:
    - Review policies and procedures on an ongoing basis with a minimal periodicity of once a year, and suggest incremental improvements (if required);
    - Propose new initiatives for improving and sustenance of ISMS to the CEO;
    - Coordinate corporate-wide information security initiatives;
    - Coordinate information security internal audits with the Audits & Compliance.
    - Coordinate external audits with certifying bodies (if any) for the period required.
    - Closure of observations/ non-conformity arising out of internal/ external audits.
    - Maintain appropriate records as required by ISMS.
    - Provide a Corrective and Preventive Actions (CAPA) report within their departments;

Coordination Responsibility

The Information Security Officer, along with department heads of CNTXT, shall be responsible:

- Ensuring policy objectives are met and responsible for supervising records generated per the security operation.
- Preparing the Information Security budget and submitting it to top management for approval.
- Being available as the key point of contact for day-to-day security implementation/issues.
- Arranging regular security audits as per management decisions.
- Provides inputs to regular internal independent audits.

Authority

The Information Security Officer, along with department heads of CNTXT, shall have the authority:

- To Oversee and maintain the Information Security Posture.
- To create additional policies, procedures, and metrics with respect to ISMS operation.

Key Skills & Competencies

The Information Security Officer, along with department heads of CNTXT, shall be verified to be competent to:

- Understand information assets.
- Understand information security and its implications.
- Understand ISO 27001 control requirements.
- Ability to interpret policy documents (internal and external) and explains to business “how to implement or demonstrate compliance”.

2.1.3 Infra Operations Person

Roles & Responsibilities:

- The IS Team shall have the responsibility of operating, monitoring, reviewing, maintaining, and improving the ISMS;
- Address the security incidents reported in the platform. Finding RCA for critical incidents and preparing incident reports to notify to Information Security Officer.
- Suggest specific initiatives to enhance information security;
- Review high-impact information security incidents with due assistance from the Engineering Team/On-Call Engineer/ Administrators;
- Work with Process Owners during the annual Risk register updates;
- Monitoring significant changes in the threat perception for information assets to include changes in technology environment;
- Ensure that security risks identified in the organization are remediated in a timely manner;
- Propose department-specific initiatives in information security to the Information Security Officer

Authority

- To inform management about any new incident/risk/vulnerability.
- Coordinate and perform necessary actions if any incident/risk/vulnerability occurs.

Key Skills & Competencies

- Understand the business need for protection.
- Understand the business 'impact' of violation.

2.1.4 Process Owners

- Process Owners are responsible for approval of procedures, templates, and other documentation relevant to their process areas and domains;

- Assist Information Security Officers in implementation and compliance with the information security procedures within their respective product departments;
- Assist Information Security Officer to implement and monitor information security processes and procedures for compliance by third parties for their respective product departments;
- Communicating the ISMS goals and requirements to their respective departments;
- Updating all the ISMS procedures as well as the risk registers and the risk treatment plan, among other ISMS documents;
- Performing the Risk Assessment, residual risks, and risk mitigation action plans working with Information Security Officer
- Support for internal and external audits; and
- Take appropriate closure actions for the observations and non-conformances.

Authority

- To raise non-conformity in any aspect of ISMS operation.
- To ensure the Operational effectiveness of respective processes.

Key Skills & Competencies

- Ability to make judgments about the 'intent, implement and effectiveness'.
- Pass a judgment and make a justification of the judgment.
- Access to the ISMS roles & responsible documents.

2.1.5 End-User Responsibilities

Employees play a critical role in information security management at CNTXT. Employees shall follow and comply with the requirements of ISMS, data security, and the applicable legal and contractual obligations. All employees covered under the scope of ISMS at CNTXT shall undertake the necessary preventive precautionary, as well as designated reactive, steps with regard to incidents. Following are the responsibilities of all employees at CNTXT:

- Shall be aware of the ISMS Policy and Objectives;
- Ensuring active participation in ISMS initiatives like ISMS training and awareness, ISMS audits, reviews, etc.;
- To report incidents/security breaches and suspected incidents on the CNTXT app;
- To understand the importance of data protection and data security responsibilities as part of their job functions;
- Maintaining the strict confidentiality of personal data and organizational data;

- To dispose of confidential and restricted information in their possession in accordance with the organization's disposal policy; and
- Taking all appropriate legal, organizational, and technical measures, in accordance with CNTXT policies, to protect the confidentiality of organizations data against accidental or unlawful disposal or accidental loss, alteration, unauthorized disclosure, and against all other unlawful forms of processing, keeping in mind the nature of such data.

Authority

- To report any new weakness/incident to the head of department/CISO.

Key Skills & Competencies

- Ability to communicate any security weakness/incident to supervisors/reporting manager or CISO.
- Ability to comply with end-user compliance requirements.

2.1.6 Third-Party Employees

CNTXT have operational dependency on third party consultants, vendor/ suppliers for its business operations.

All external parties (i.e., third-party employees, vendors/ suppliers, consultants, interns, customers, etc.) must participate and assist CNTXT in undertaking the necessary precautionary/preventive, as well as reactive, steps towards controlling IS breaches.

Following are the indicative responsibilities of all external parties at CNTXT

- To understand and follow CNTXT ISMS Policy (when accessing CNTXT information systems/ CNTXT assets);
- Ensuring active participation in ISMS initiatives like training and awareness, audits, reviews, etc. (where applicable); and
- Ensuring instant communication and reporting breaches or suspects on the CNTXT app.

3. Segregation of Duties

- Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets;
- Care has be taken that no single person can access, modify or use assets without authorization or detection;
- The following principles will be followed:

- Persons involved in operational functions must not be given additional responsibilities in system administration processes and vice versa;
- Persons involved in testing processes must not be given additional responsibilities in system administration processes and vice versa; and
- The responsibility for performing a security review of the system or process has to be completely independent from the roles and responsibilities for developing, maintaining, and using the system or method.

- The below guidelines shall be considered to ensure the segregation of duties:
  - Human Resource (HR) department, in consultation with the Department Head who has prepared the Job Description (JD), shall be responsible for identifying the roles and responsibilities associated with every individual;
  - Wherever feasible, personnel involved in software/application development shall not be given additional responsibilities like testing or deployment in production, etc.;
  - Function Heads shall ensure that there are separate teams to review, administer, and monitor the servers and network devices, adhering to the segregation of duties principle;
  - The log review administrator should be different from the administrator of the systems;
- In those instances where duties cannot be entirely segregated, mitigating or compensating controls must be established, such as:
  - Audit trails - In the absence of adequate segregation of duties, good audit trails may be an acceptable compensating control. Audit trails help recreate transaction flow from the point of origination to its existence. Good audit trails should be enabled to provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated.
  - Supervisory reviews—Supervisory reviews may be performed through observation and inquiry or remotely.
  - Independent reviews— To compensate for mistakes or intentional failures by following a prescribed procedure, independent reviews are recommended. Such reviews can help detect errors and irregularities.

4. Document Security Classification

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

5. Non-Compliance

Compliance with this document shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the document owner. Any staff member found to be in violation of this document 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. Responsibility

The Information Security Manager is primarily responsible for ensuring adherence to the policy. Department heads are responsible for the implementation of corrective/preventive action.

7. Schedule

This document should be reviewed at least on an annual basis or earlier whenever deemed necessary due to required updates or changes.

End of ISMS Information security Roles and Responsibilities. 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