ISMS Manual

Version 1 - Approved by Youssef Ouyhya

Contents

1. Purpose

This document details the Information Security Management System (ISMS) of CNTXT FZCO (hereafter CNTXT). This document is the framework for designing, implementing, exercising, and maintaining the ISMS. The manual references the CNTXT's information security initiatives.

This manual provides regulators and other interested parties with appropriate information about the CNTXT's information security management objectives and initiatives undertaken.

The information security policies documented by CNTXT apply to all CNTXT information asset users. These policies apply to all Information Systems (IS) environments operated by CNTXT. The term "IS environment" defines the total environment and includes, but is not limited to, all documentation, personnel, hardware (e.g., desktops, etc.), software, and information.

2. Organization Overview

2.1 About CNTXT

We specialize in meticulously preparing, cleansing, and structuring your data to unlock its full potential, ensuring it meets the highest standards for accuracy and usability. By making your data AI-ready, we empower you to harness cutting-edge technologies, drive insightful analytics, and achieve transformative business outcomes.

2.2 Vision & Goals

In today's rapidly evolving digital landscape, data is the lifeblood of innovation and competitive advantage. At CNTXT, our mission is to transform your raw data into a powerful asset, ready to fuel the most advanced AI solutions. We specialize in meticulously preparing, cleansing, and structuring your data to unlock its full potential, ensuring it meets the highest standards for accuracy and usability. By making your data AI-ready, we empower you to harness cutting-edge technologies, drive insightful analytics, and achieve transformative business outcomes. Join us on a journey to revolutionize how you leverage data, turning complex challenges into seamless, intelligent solutions.

3. Terms & Definitions

- **Asset:** Anything valuable to CNTXT.
- **Audit:** Independent review of an activity or process to determine if it has functioned as intended.
- **Audit Trail:** The audit trail represents the path that a particular transaction/ transaction cycle takes in the system and can be generated by way of a report/log of events describing the detailed history of

system activities and processing. Audit trails are generated with definite control objectives, which reflect details of activity, process, and events to be monitored.

- **Confidentiality:** relates to the protection of sensitive information from unauthorized access.
- **Integrity:** relates to the accuracy and completeness of information, as well as to the validity of information in accordance with business values and expectations.
- **Availability:** relates to information being available when required by the business process. It also deals with the safeguarding of necessary resources and associated capabilities.
- **Control:** Means of managing risk, including policies, procedures, guidelines, practices or Organizational structures, which can be of administrative, technical, management, or legal nature.
- **Data classification:** Grouping of CNTXT's entire information and business data into such categories which denote the criticality and sensitivity of the information. Data classification aims at achieving three major attributes of information, viz. Confidentiality, integrity, and availability.
- **Information:** Applies to any storage, communication, or receipt of knowledge, such as fact, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.
- **Information Asset:** Information that has value to our company, including people, paper, Logical (Information), Physical, Software and Service, and Site.
- **Information Asset Custodian:** Employees responsible for maintaining the information protection measures defined by the information asset owner.
- **Information Asset Owner:** Employees responsible for creating and using information assets. Asset owners decide the security requirements for the asset.
- **Information Processing Facilities:** Any information processing system, service, or infrastructure, or the physical locations housing them.
- **Information Security:** Preservation of confidentiality, integrity, and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.
- **Information Security Management System (ISMS):** That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security. The management system includes Organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources.
- **Information System:** The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.
- **Media:** All devices that can electronically hold and store information. These include CDs, DVDs, tapes, and portable hard disks and any development from these.
- **Policy:** Overall intention and direction as formally documented and expressed by management.
- **Standard:** Standard is a definite way of doing things, a series of steps to an end, or a set of established forms and methods for conducting legal and business affairs. The standards substantiate ways and means of implementing policies.

- **Risk:** Combination of the likelihood of an event and its impact.
- **Risk Acceptance:** It is the decision to accept a risk.
- **Risk Analysis:** The systematic use of information to identify sources and to estimate the risk.
- **Risk Management:** Coordinated activities to direct and control CNTXT with regard to risk.
- **Safeguard:** This is defined as the mechanism by which a control may be implemented, optionally with others, to reduce or eliminate an identified threat.
- **Security Event:** An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
- **Security Incident:** A single or a series of unwanted or unexpected information security events that have a significant likelihood of compromising business operations and threatening information security.
- **Statement of Applicability:** The document describing the control objectives and controls that are relevant and applicable to the organization's ISMS.
- **Third Party:** That person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
- **Threat:** Threat is the potential cause of an unwanted event that may result in harm to the CNTXT and its assets.
- **Virus:** A computer virus is a piece of malicious software designed to attach itself to other programs and to replicate itself into other programs, ultimately very possibly infecting every program in a system. There is also a variant known as a macro virus, which attaches itself to the macros, which are a part of some word processor and spreadsheet programs. Other malicious software goes by such names as worms, Trojan horses or time bombs. These can all be very damaging to a system but are free standing rather than replicating attachments.
- **Vulnerability:** Vulnerability is defined as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

4. Context of the Organization

4.1 Understanding the organization & its context

CNTXT has developed an organizational governance structure, and has defined policies, strategies and well-defined roles and responsibilities to ensure that strategic objectives are met. Information Security Management System (ISMS) is designed to be a subset of the overall organizational governance framework. CNTXT has taken steps to determine risks and opportunities which could impact the goals and objectives.

CNTXT has determined external and internal issues that are relevant to its purpose, and that may affect its

ability to achieve the intended outcome(s) of its Information Security Management System (ISMS).

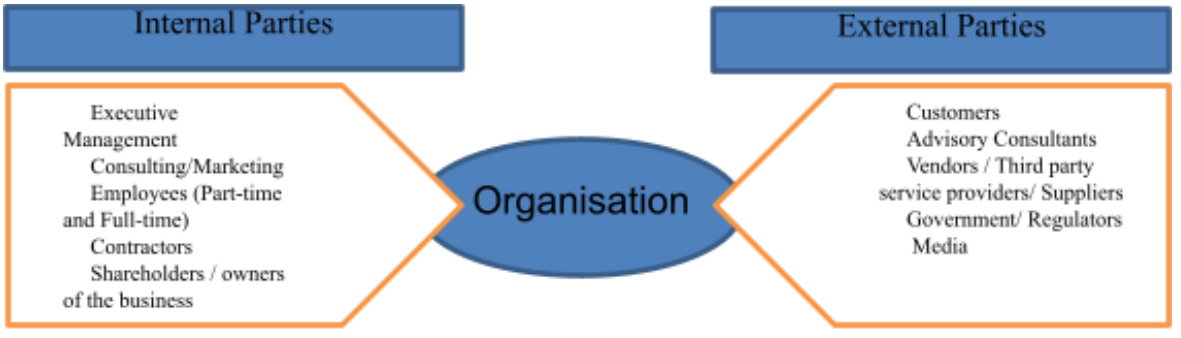
CNTXT has determined the internal and external interested parties and their needs and expectations with respect to ISMS. The requirements of these interested parties are accommodated within the ISMS approach and the scope of ISMS. Some of the internal and external interested parties who have an impact on CNTXT ISMS include:

- Internal Issues:
  - Availability of reliable qualified and competent workforce;
  - Stability of work force and Staff retention and congenial work culture;
  - Opportunities to improve technology;
  - Expansion of Customer base/contractual arrangements/SLA with suppliers; and
  - Inadequate awareness towards Information Security.

- External Issues:
  - Compliance with the guidelines/ directives, regulations, and Laws;
  - Compliance with the requirements and regulations required by the clients and as agreed between CNTXT and Client as part of MSA;
  - Overall economic performance of the country;
  - Customer demographic;
  - Protection of assets against damage due to external factors like cyber-attacks, unrest and natural calamities; and
  - Competitive business environment.

4.2 Understanding the needs and expectations of interested parties

CNTXT shall identify the interested parties, i.e., individuals or organizations that can influence or can be affected by CNTXT's information security. The needs and expectations of the interested parties to adequately enhance the security or meet disaster recovery requirements shall be determined. CNTXT has identified the following requirements of internal/external interested parties for its Information Security Management system:



Interested Parties	Internal/external	Requirements
Executive Management	Internal	• Minimal business interruptions • Business growth • Maintenance of brand value and reputation • Ensuring customer satisfaction • Ensuring continued relationships with key partners and vendors • Adherence to legal & regulatory requirements • Adherence to contractual requirements
Consulting/Marketing Group	Internal	• Business growth and profits • Maintenance of brand value and reputation • Ensuring customer satisfaction • Minimal business interruptions
Employees/ staff	Internal	• Life safety • Congenial work environment • Continuity of employment • Security of personal assets from damage or destruction
Government/ Regulators	External	• Adherence to all legal and regulatory obligations • Timely and adequate submission of evidences of compliance as per mandate and as requested by the governing bodies • Support government and law enforcing agencies in any investigation
Customers	External	• Continued service delivery • Assurance of security of personal information from leakage or misuse • Quality of service • Availability of critical business information and application

Interested Parties	Internal/external	Requirements
Media	External	• Ensuring that the information supplied is correct and verified by a reliable source
Vendors/ Suppliers	External	• Timely and adequate communication of security requirements • CNTXT shall enforce and meet the information security requirements of its vendor's information and know-hows. • Ensuring changes to contractual terms are communicated timely.
Legal bodies	External	• Compliance with applicable legal requirements such as Fire NOC, building permits, etc.

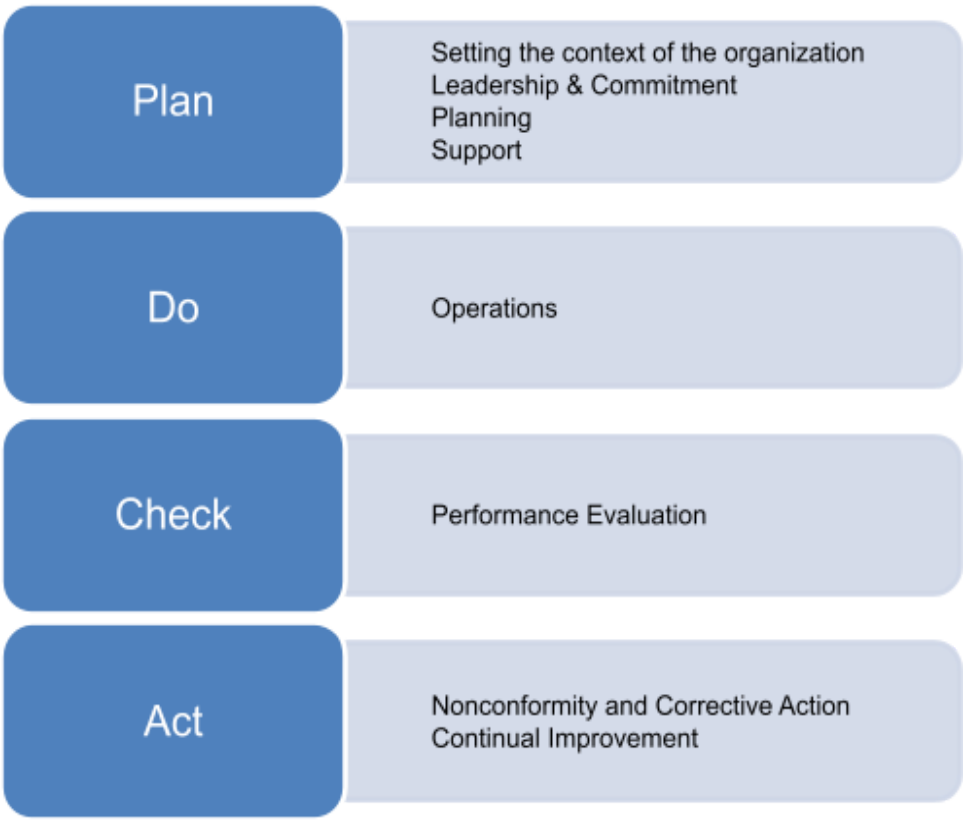
CNTXT shall identify legal & regulatory requirements for compliance and maintains them as a Legal and Contractual Requirements Register.

4.3 Scope of Information Security Management System

The scope of the Information Security Management System at CNTXT applies to infrastructure, applications, and systems that ensure the delivery of its product or services to its customers. It also includes activities that hold, obtain, share, or manage customer and business data; and the business functions of HR, Engineering & Product Management, Customer Support, Sales & Marketing, and Finance. This is in accordance with the ISMS Scope document.

4.4 Information Security Management System

CNTXT has designed its ISMS framework based on the guidelines provided by the ISO 27001 standard and industry best practices. CNTXT shall develop, implement, maintain and continually improve the ISMS.



5. Leadership

5.1 Leadership & Commitment

- CNTXT management will ensure that: ISMS policy and ISMS objectives compatible with the strategic direction of the organization are established.
- The requirements of the ISMS are integrated within CNTXT's business and operational processes.
- Roles, responsibilities, and authorities for information security management are defined, and competent resources are nominated for those roles.
- The importance of meeting information security management system objectives, conforming to the information security policy, its responsibilities under the laws & regulations and the need for continual improvement is communicated to all employees and third party contractors.
- Sufficient resources are provided to establish, implement, operate, monitor, review, maintain and improve the ISMS.
- Personnel to contribute to the effectiveness of the ISMS.
- Ensuring that the information security management system achieves its intended outcome(s).
- Continual improvement of ISMS is promoted in the organization.
- Other relevant management roles are supported, there by demonstrating their leadership as it applies to their areas of responsibility.

5.2 Policy

CNTXT's objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions. The Senior Management is committed to an effective Information Security Management System in accordance with its strategic business objectives. To that end, CNTXT shall:

- Ensure Confidentiality, Integrity, and Availability of Information Assets by adequately protecting the information and information systems against unauthorized access, modification, and alteration.
- Develop and implement Information Security Management System in order to protect the organization's information assets from various internal and external threats.
- Continually monitor and improve the effectiveness of the Information Security Management System to improve the security posture.
- Commit to comply with regulatory, legal and business requirements.
- Ensure security awareness and competency amongst associates to enable them to meet their security obligations.
- Provide a framework to manage and handle security weaknesses, breaches, violations and business disruptions.
- Develop and maintain a security conscious culture within organization.
- Communicate all pertinent security policies to Employees and other interested parties as applicable.
- Ensure that information security Policy is in line with the purpose of the organization.

The relevant policies and procedure documents are made available and communicated as a document to all the interested parties (internal and external) to the organization. The policy will be communicated to all internal employees, whenever there is a new version released and periodically. For internal and appropriate external parties, the policy requirements may be communicated to them in any of the following means:

- Emails
- Contractual requirements
- Training sessions
- Internal team meetings

5.3 Organizational roles, responsibilities and authorities

CNTXT has defined organizational roles and responsibilities for ISMS. Please refer ISMS Roles and Responsibilities document.

6. Planning

6.1 Actions to address risk and opportunities

6.1.1 General

CNTXT shall perform Risk and Opportunities analysis for all the external and internal interested parties identified in Section 4.2 of the ISMS manual. The risk and opportunities analysis performed shall ensure that the ISMS achieves its intended outcomes, prevents, or reduces undesired effects, and achieves continual improvement through the following activities:

- Identifying the applicable threats and vulnerabilities;
- Formulating an action plan to address all the risks and opportunities identified;
- Integrating the action plan into the ISMS processes and tracking them to completion;
- Evaluating the effectiveness of the action plan; and
- Reviewing and updating the risk and opportunities analysis annually to include any changes to the interested parties and their associated risks and opportunities.

6.1.2 Information Security Risk Assessment

Risk assessment is a process of identifying, quantifying, prioritizing risks against objectives relevant to the organization. The result of the risk assessment exercise determines the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

Risk assessment will include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk acceptance criteria to determine the significance of the risks (risk evaluation) and implementing controls to mitigate the risk (risk treatment plan)

6.1.3 Information Security Risk Treatment

CNTXT shall define and apply an information security risk treatment process to:

- Select appropriate information security risk treatment options, taking account of the risk assessment results and risk owners' decision;
- Determine all controls that are necessary to implement the information security risk treatment option(s); and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls
- Establish information security objectives and plan to achieve them.

6.1.4 Objectives

The overall objective of CNTXT towards Information Security is to ensure protection of its information systems against damage or destruction and unauthorized disclosure or changes, whether it is accidental or deliberate.

In addition, the information systems should comply with relevant laws and regulations.

Objective	Mapping to the IS Policy	Measurement criteria	Responsibility	Evaluation schedule
To have a documented and approved information security policy	The information security Policy is in line with the purpose of the organization.	The policy should be reviewed annually	Information Security Officer	Continuous through Sprinto App (ISMS monitoring tool)
To identify the information assets, to understand their vulnerabilities and the threats that may expose them to risk, through appropriate risk assessment	Create mechanisms to identify and review the risk and impact of threats and breaches. Ensure confidentiality, Integrity and availability of Information Assets.	100% coverage of functions in annual risk assessment	Information Security Officer	Continuous through Sprinto App (ISMS monitoring tool)
To ensure that identified risks are mitigated through adequate controls as documented in the risk treatment plan	Create mechanisms to identify and review the risk and impact of threats and breaches.	Less than 10% deviation in implementation as per RTP	Information Security Officer	Continuous through Sprinto App (ISMS monitoring tool)
To ensure annual information security awareness training of all employees and key vendors	Create and maintain a security conscious culture within organization.	100% coverage of all employees and vendors	HR	Continuous through Sprinto App (ISMS monitoring tool)
To ensure that security controls implemented are adequate and no P1	Develop and implement Information Security Management System in order to reasonably and	Not more than three major information security incidents	Information Security Officer	Continuous through Sprinto App (ISMS

Objective	Mapping to the IS Policy	Measurement criteria	Responsibility	Evaluation schedule
information security incident (IT) occurs	effectively protect organization's information assets from various internal and external threats.			monitoring tool)
To ensure timely compliance to all legal and regulatory requirements	Commit to compliance with regulatory, legal, and business requirements.	Non Compliance with Legal and Regulatory requirements	Information Security Officer	Continuous through Sprinto App (ISMS monitoring tool)
To ensure that management reviews are conducted as per the defined frequency	Continually monitor and improve the effectiveness of the Information Security Management System.	Annual management review meeting should be planned	Information Security Officer	Continuous through Sprinto App (ISMS monitoring tool)

6.1.5 Planning

CNTXT's Management is committed to instituting, implementing, and improving Information Security Management System. The management exhibits its commitment by:

- Establishing information security objectives.
- Providing sufficient resources for the implementation and improvement of security systems and controls.
- Establishing and communicating the roles and responsibilities for the smooth operation of ISMS.
- Communicating to all the employees the importance of meeting information security objectives, conforming to the information security policy, and the need for continual improvement of the implemented ISMS.
- Defining the criteria for acceptance of risk and review the exceptions.
- Conducting periodic reviews of the ISMS to ensure that gaps (if any) are identified, and remediation plans (if applicable) are in place.

- Establishing a framework to promote timely reporting of security events by identifying weaknesses, which might impact the organization's ISMS or result in any disruptive incidents.
- Monitoring the prioritization of funds to support ISMS activities.

7. Support

7.1 Resources

CNTXT will determine and provide resources needed to:

- Establish, implement, operate, maintain, and improve ISMS.
- Ascertain that all the business requirements are meeting the procedures and policies laid down under ISMS.
- Identify and address legal/ regulatory requirements and contractual security obligations.
- Maintain adequate security by correct application of all implemented controls.
- Carry out reviews when necessary, and to react appropriately to the results of these reviews.
- Improve the effectiveness of ISMS, where required.

7.2 Competence

CNTXT shall ensure that all the personnel taking up ISMS roles are competent.

7.3 Awareness

CNTXT shall ensure that all personnel who are doing work under the organization and the ones who are assigned responsibilities defined in the ISMS are:

- Aware of Information Security Policy.
- Aware of their contribution to the effectiveness of the ISMS, including the benefits of information security and improved management performance.
- Provided required training wherever needed and, if necessary, employing competent personnel to satisfy these needs.
- Imparted with Security Awareness training and assessed periodically for awareness
- Evaluated against the effectiveness of the training provided and actions taken.
- Required to submit records of education, training, skills, experience, and qualifications.

CNTXT management will also ensure that all relevant personnel is aware of the importance of their information security activities and how they contribute to the achievement of the ISMS objectives. The management shall also ensure that all new joiners undergo basic Information Security awareness training during induction.

7.4 Communication

CNTXT shall follow the appropriate communication standards to establish and implement an effective communication framework for internal/ external interested parties of CNTXT as identified in the section 4.2 of the ISMS Manual.

7.5 Documented Information

7.5.1 General

ISMS at CNTXT has been fully documented and approved by the management. The documentation includes:

- Information Security Manual;
- Information Security Policy;
- Information security management system policies;
- Statement of Applicability;
- Risk registers / Risk Treatment Plans; and
- Other records as per operational requirements.

The policy and procedure documents have been distributed/ made available to relevant employees of CNTXT under the scope of ISMS. It enables staff to remain aware of their responsibilities and the organization's security policies while providing them with basic guidance to manage security in accordance with the documented procedures.

7.5.2 Creating and updating

Documents / Records will be established and maintained (in hard copy or soft copy) to provide evidence of conformity to requirements and the effective operation of the ISMS. Access to the records shall be controlled to people who are authorized to have an access. CNTXT shall take account of any relevant legal requirements in case of retention of specific records.

7.5.3 Control of Documented Information

Documented information required for implementing, managing, monitoring, and improving the ISMS at CNTXT will be protected and controlled. This shall involve:

- Approval of documents for adequacy, prior to them being issued.
- Review and update of documents as necessary and re-approval of documents.
- Ensuring that changes made to the document and the current revision status of documents are easily identifiable.
- Ensuring that the most recent versions of relevant documents are available at points of use.

- Ensuring that documents remain legible and readily identifiable.
- Ensuring that documents of external origin are identified.
- Ensuring that the distribution of documents is controlled as per the document classification.
- Preventing unintended use of obsolete documents.
- Applying suitable identification to them if they are retained for any purpose.

8. Operations

8.1 Operational Planning and control

CNTXT shall plan, implement and control the processes needed to meet information security requirements and to implement the actions required to address the risk and opportunities identified in section 6.1 of this document. This shall be done by preparing an action plan to address each risk or opportunity and assigning an action owner to each plan.

CNTXT shall maintain documented information to ensure that processes are being accepted to achieve expected outcomes.

CNTXT shall control and monitor changes to information processing facilities and adopt actions necessary to mitigate adverse effects.

8.2 Information Security Risk Assessment

CNTXT shall perform information Security risk assessments at least once in a year. Risk assessments shall also be performed in case of a major change in CNTXT services or in case of a major information security incident.

The procedure to carry out risk assessments is implemented, and CNTXT shall retain documented information on the information security risk assessments.

8.3 Information Security Risk Treatment

CNTXT shall implement the information security risk treatment plan as per the risk assessment policy. CNTXT shall retain documented information on the information security risk treatment.

9. Performance Evaluation

9.1 Monitoring, Measurement, Analysis & Evaluation

CNTXT shall evaluate the information security performance and the effectiveness of the Information security management system. This shall be done as a part of CNTXT's Internal Audit.

9.2 Internal Audit

Internal ISMS audits at CNTXT will be conducted annually to assess the efficiency of implemented ISMS and to determine the controls/ procedures of ISMS are effectively implemented, maintained, and conform to relevant legislations, standards, and security requirements and perform as expected. The audit will be conducted to determine whether the control objectives, implemented controls, processes, and procedures of the ISMS:

- Takes guidance from the ISO 27001 standard and relevant legislation or regulations, and license conditions.
- Conform to the identified information security requirements.
- Are effectively implemented and maintained.
- Perform as expected.

Continuous monitoring of the effectiveness of ISMS controls is done, and this information can be leveraged to conduct the Internal Audit.

9.3 Management Review

The defined management for CNTXT will review the organization's ISMS at least once per year and when significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. This management review will include assessing opportunities for improvement and the need for changes to the ISMS, including the Policy and Objectives.

9.3.1 General

The management review meeting by the Information Security Officer and department heads is held once a year to ensure ISMS's continuing suitability, adequacy, and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the Information Security policy and objectives. The results of the review shall be clearly documented, and records shall be maintained.

9.3.2 Review Input

The input to a management review shall include information on

- Results of ISMS audits and reviews that have been conducted;
- Feedback from interested parties;
- Techniques, products, and procedures, which could be used in/by the organization to improve the ISMS performance and effectiveness;
- Security incidents reported;

- Risk assessment results and status of risk treatment plans;
- Status of the corrective actions that have been identified;
- Security reports and recommendations by Information Security consultants;
- Vulnerabilities identified during risk assessment exercise;
- Follow-up actions from previous management reviews;
- Any changes that could affect the ISMS; and
- Recommendations for improvement.

9.3.3 Review output & ISMS improvement

The output from the management review shall include any decisions and actions related to the following:

- CNTXT shall constantly work towards ensuring the effectiveness of controls
- CNTXT shall also consider review based on service requirements or security requirements
- Business processes affecting the existing service requirements
- Regulatory or legal environment
- Levels of Risk and/or levels of risk acceptance
- Corrective actions or preventive actions based on the review/audit findings and results, various security incidents reported, suggestions and other relevant changes
- Resource Needs

10. ISMS Improvement

10.1 Non-Conformity & Corrective Action

CNTXT will take actions to eliminate the causes of any reported non-conformities associated with the documented and implemented ISMS in order to prevent its recurrence. These actions are known as corrective actions. Corrective actions can be identified from audit /review results, any feedback or suggestions received, or security incident reports. The focus of corrective action is to identify similar occurrences in similar systems and resolve them. Root cause analysis shall be performed for all major and minor non-conformities reported in internal/external audits, medium/high risk identified in the Risk and Opportunities tracker, and critical level security incidents.

CNTXT will strive to identify potential non-conformities and their causes or changes in the business/ operating environment, which may affect the implemented system, and take actions to safeguard against them (i.e., risk analysis).

Non-Conformity and Corrective Action plan shall be developed and implemented by respective departments/process owners. The Information Security Officer shall be responsible for tracking the progress of

the corrective actions.

10.2 Continual Improvement

The enhancement and continual improvement of the implemented Information Security Management System at CNTXT is accomplished through security policy, security objectives, and audit results, analysis of monitored events, corrective actions, and management review.

10.2.1 Continually Improve the ISMS

- CNTXT will implement the improvements identified by the audit committee/ management to the ISMS, and the same will be communicated to all interested parties.
- Follow up after management review of ISMS.
- Improvement of ISMS will also take into account changing business environments as well as the identification of the new set of threats and their implications on business.
- Learnings from information security incidents:
    - An incident may lead to unavailability of following basic components, which supports information security:
        a. Information
        b. People
        c. Technology
        d. Site
        e. Service
    - Any unavailability of the above may result in business disruption.
    - CNTXT shall establish an Incident Management procedure to address any event/incident that may lead to information security disruption. All such events that result in the unavailability of one or more of the above factors shall be studied and analyzed in detail to identify the following learning:
        a. Root cause analysis shall only be performed for critical category incidents.
        b. The corrective actions that need to be taken to minimize the damage to business from any such event.

11. Document Security Classification

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

12. 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.

13. Responsibilities

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

14. Schedule

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

End of ISMS Manual. 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