ISMS INFORMATION SECURITY POLICY

NSEIT Ltd

RELEASE NOTICE

Document Name	Information Security Policy
Document Type	ISMS
Version	20.1
Release Date	11-March-2024
Document Number	ISMS/INFSECPOL VER 20.1

Reviewed by	Lakshmi Ekbote	**Approved By**	Atul Shukla
Reviewed Date	04-Mar-2024	**Approved Date**	11-March-2024

COPYRIGHT NOTICE

REVISION HISTORY

No.	Version	Prepared or Revised by	Reason for Preparation or Revision	Reviewed By	Approved By	Release Notice
1	1.0 Draft 1.0	ISO 27001 Implementation team	For use	CISO	CISO	NA
2	1.0 Draft 2.0	CISO	High-level policy statements instead of detailed policies.	CISO	CISO	NA
3	1.0 Draft 3.0	CISO	Incorporation of review comments	CISO	CISO	NA
4	1.0 Draft 4.0	Steering Committee	Incorporation of name of members of security organization and their responsibilities	CISO	CISO	NA
5	1.0	Information security Forum	For use	CISO	CISO	22/07/2005
6	2.0	BS 7799 Implementation team	Incorporating the changes suggested by the BSI assessors	CISO	CISO	11/09/2005
7	3.0	ISO 27001 Implementation team	Incorporated changes to comply with BS 7799 - ISO 27001 migration	CISO	CISO	05/09/2006
8	4.0	ISO 27001 Implementation team	Incorporated changes to comply with ISO 27001	CISO	CISO	19/04/2007
9	5.0	ISO 27001 Implementation team	Incorporated review changes to comply with ISO 27001	CISO	CISO	01/04/2008
10	6.0	ISO 27001 Implementation team	Incorporated changes to organization chart	CISO	CISO	01/09/2008

11	7.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	15/09/2011
12	8.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	20/09/2012
13	9.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	23/09/2013
14	10.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	09/09/2014
15	11.0	ISO 27001 Implementation team	Incorporated changes to comply with ISO 27001:2013. Steering Committee members changed	CISO	CISO	08/07/2015
16	12.0	ISO 27001 Implementation Team	Made changes in company logo, name version and CISO name	S R Sharma	CISO	01/08/2016
17	13.0	ISO 27001 implementation Team	Updating in Security Organization	S R Sharma	CISO	13/12/2016
18	14.0	ISO 27001 Implementation Team	NSEIT Logo change	Mayuri Rachacha	CISO	24/07/2018
19	15.0	ISO 27001 Implementation Team	Incorporated Changes to comply with ISO 27001:2013 Steering Committee member	CISO	CISO	23/06/2019
20	16.0	ISMS 27001 & 27002 Implementation Team	Incorporated changes to comply with ISO 27001:2013 & 27002:2013 Steering Committee member	Sheetal Gupta	CISO	16/03/2020
21	17.0	ISMS 27001 & 27002	Annual Review & Steering committee members update.	Sheetal Gupta	CISO	25/04/2020

		Implementation team				
22	18.0	ISMS 27001 & 27002 Implementation Team	Annual Review & Steering committee members update	Sheetal Gupta	CISO	02/04/2021
23	19.0	ISMS 27001 & 27002 Implementation Team	Annual Review	Quality Team	CISO	03/01/2022
24	20.0	Revised Standards ISO 27001:2022	Updated control	Priyanka Nambissan	Atul Shukla	14/03/2023
25	20.1	Revised Standards ISO 27001:2022	Annual Review	Lakshmi Ekbote	Atul Shukla	11/03/2024

Table of Contents

1. Introduction

The security policy of NSEIT has been developed to set up an Information Security Management System (ISMS) through which IT systems may be safeguarded. This document details the policies adopted by NSEIT to assure an adequate level of protection and control for IT systems whether maintained in -house or otherwise. The security policy is expected to ensure that:

IT Systems operate effectively and accurately, without compromising the confidentiality, integrity and availability of NSEIT's critical assets. There are appropriate technical, personnel, administrative, physical, environmental, and telecommunications safeguards in IT systems. The continuity of the operations of IT systems that support critical functions is preserved. NSEIT's ISMS will provide reasonable and acceptable assurance that its IT systems provide adequate protection to sensitive and classified information, that data and software integrity is maintained; and, that unplanned disruptions of processing will not seriously impact business operations.

This document contains the policies that represent management's commitment to ISMS. It is intended to provide functional custodians and individual system owners with a detailed single-source reference document, which will be updated as new policies, procedures, techniques, methodologies or program requirements are developed and issued. Due to the complexity of the ISMS requirements, the policy section of this chapter is divided into sub-sections that present policies by specific subjects.

2. Purpose

The Security Policy of NSEIT complies fully with the ISO 27001 standard and communicates policies for the protection and control of IT systems directly or indirectly relating to the activities of NSEIT. The security policy has been developed in accordance to the control objective of the **ISO 27001:2022 control A.5.1.-Policies for information security.**

The purpose of this document is to define all policies and responsibilities for the establishment, implementation, maintenance and oversight of the ISMS within NSEIT. All NSEIT employees should be aware of this policy, the need to ensure appropriate secure and confidential handling of all personal and business sensitive information and their responsibilities in maintaining information security.

Failure by any employee of NSEIT to adhere to the policy and its guidelines will be considered to be a serious breach that may result in disciplinary action. If for any reason any employee believes that it is not possible to meet the policy and associated guidelines this must be brought to the attention of the Chief Information Security Officer so that relevant action may be agreed and notified to the Information Security Forum of NSEIT.

Note: Security breaches may result in disciplinary action.

3. Definition of Information Security Management System

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected."
Information in this policy includes data within NSEIT and its customer's confidential information as applicable within the contract between parties.

Information security aims at protecting information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investment and business opportunities. The three basic components in Information Security Management are.

Confidentiality: Ensuring that information is accessible on to those authorised to have access.
Integrity: Safeguarding the accuracy and completeness of information and processing methods.
Availability: Ensuring that authorized users have access to information and associated assets when required. A system designed to meet the three basic components of Information Security and to provide protection to assets from vulnerabilities and threats is **Information Security Management System.**

4. Management Intent

The management of NSEIT endeavours to support the establishment of security systems, set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of a Security Policy across the organization and user groups.

5. Background and Authority

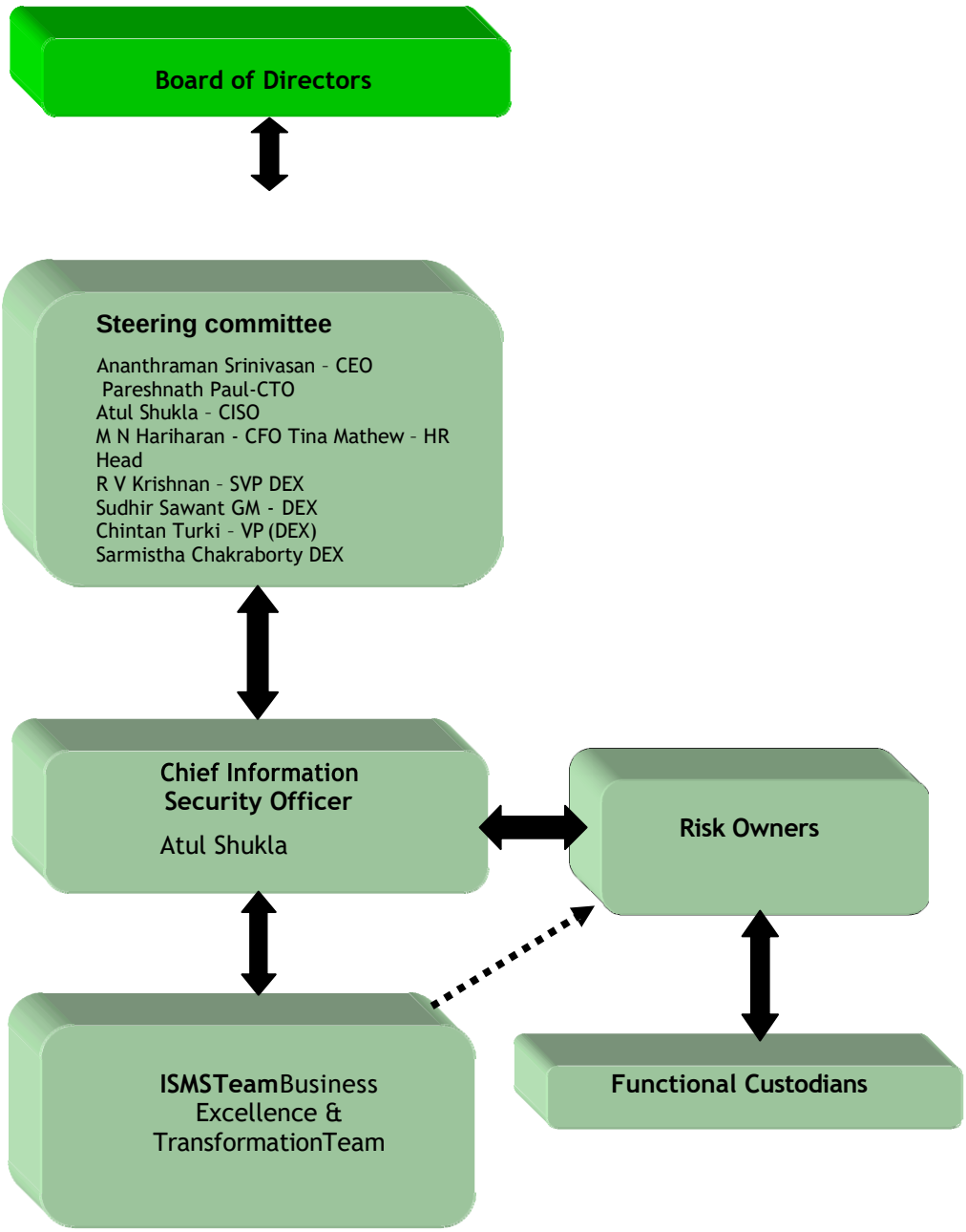
NSEIT has established an ISMS in order to have adequate protection and control of its IT Systems and to get ISO 27001 certification. The ISMS mandates the establishment of an Information Security organization with well-defined roles and responsibilities for ensuring information security in all its departments. The individuals appointed to positions with IT security responsibilities are accountable for compliance with all policies related to the assigned responsibilities. The Security Policy is developed in compliance with the ISO 27001:2022 Part - II. Refer the ISMS scope document and the Security Organization document for further details.

6. Scope

The policy scope is in line with the scope of ISMS for NSEIT. The scope of ISMS for NSEIT is limited to its offices (Trade Globe & Trade Star) in Mumbai, NSEIT Offices at Chennai (Guindy & Vadapalani) and covers the software development (Products, Projects and Services), the Enterprise Management Services (Managed services, Software testing services and Consulting services), Digital Examination services, Support services (HR, IT and Admin and other ancillary services related to the above. Unless explicitly mentioned, any reference to NSEIT in this document pertains only to the Mumbai operations (Trade Globe & Trade Star) of NSEIT. The policies contained in this document are applicable to all IT resources of NSEIT that are above a certain level of sensitivity, whether maintained in-house or otherwise. These policies are mandatory on all

organizational units, employee's contractors, and others having access to and/or using the IT resources of NSEIT. These policies apply to all IT resource currently in existence and to any new IT resource acquired after the effective date of this policy document.

7. Information Security Roles & Responsibilities



For further details kindly refer annexure I of this document.

8. Risk

Any security measure must be viewed as protection against a risk of an event occurring and the impact thereof. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

The Threat of something damaging the confidentiality, integrity or availability of information in systems or manual records.

The **Vulnerability** of an asset or a system that can be effectively exploited by a threat thereby resulting in damage. The **Impact** that such a threat would have if it occurred. All employees should consider the risks associated with information systems and the information in them, as well as information in manual records.

All employees are responsible for reporting any apparent shortcomings of security measures currently employed. These shortcomings must be reported to the respective department's functional custodian.

9. Policy

The following policies are in place for maintaining an adequate level of protection and control for IT systems at NSEIT.

9.1 Access Control Policy

Only authorized users are granted access to information systems, and users are limited to specifically defined, documented and approved applications and levels of access rights. Access to systems will only be granted where there is a clearly established business need, which is consistent with the roles and responsibilities of those granted access. Computer and communication system access control is to be achieved via user IDs that are unique to each individual user to provide individual accountability.

9.2 Acceptable Usage of IT Resources Policy

The acceptable usage of computing/communicating resources must be defined and authorized. The domains wherein such guidelines are defined are: Systems & Networks, Email & Communications. Inappropriate use exposes NSEIT to risks including virus attacks, compromise of network systems and services, and legal issues. The objective of this policy is to outline the acceptable use of computer/ network equipment at NSEIT.

9.3 Acceptable Encryption Policy

It is recommended to use proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA as the basis for encryption technologies. The use of proprietary encryption

algorithms is not all owed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Chief Information Security Officer. The objective of this policy is to prevent unauthorized disclosure of information and non-infringement of IPR.

9.4 Audit Trail Policy

The audit trails must be enabled for the critical systems of NSEIT. This policy is applicable to administrative as well as technical systems that are used in NSEIT. There should be a mechanism for recording and reviewing the same. The objective of this policy is to control the use of the critical systems of NSEIT and provide data for analysing any information security breaches related to the system.

9.5 Backup Policy

In order to safeguard information and computing resources from various environmental and other threats, systems and procedures should be developed and implemented by NSEIT for ensuring that information remains consistent and available when required.
The purpose of this policy is to define the guideline for performing periodic computer system backups to ensure that mission critical data and archives are adequately preserved and protected against data loss and destruction.

9.6 Change Management Policy

Change management requirements must be applied whenever the NSEIT's system software application software, databases, hardware, network or data are changed or modified. The objective is to streamline the process of managing changes to critical systems/processes with no adverse impact on productivity.

9.7 Clear Desk, Clear Screen Policy

The employees of NSEIT must follow a clear screen clear desk policy at all times.
The objective of this policy is to prevent unauthorized disclosure of information at the workplace.

9.8 Corporate Communication Policy

The flow of confidential & sensitive information of an organization to the outside world should be restricted & controlled. The objective is to define processes & controls for ensuring that all corporate communication between NSEIT & the outside world occurs in a secure manner without adversely affecting the business prospects of NSEIT.

9.9 Dial-Up (data card) Policy

NSEIT employees and authorized third parties (customers, vendors, etc.) can use dial -in with VPN (virtual Private Network) connections to gain access to the corporate network. Use of such communication must be subject to approval of the CISO. Dial-in with Data card using VPN access should be strictly controlled, using strong password authentication. (In accordance with NSEIT's password policy). Use of Dial-up with Data card using VPN

connections for internet access is prohibited. However Data card with VPN may be allowed to be used on a case-to-case basis, subject to approval from the CISO. The objective of this policy is to control and manage the access to NSE its network through dial-up lines, Data cards etc.

9.10 Email Policy

The email facilities of NSEIT should be used only for official purposes for communication between NSEIT stakeholders (Employees, management, partners, customers etc). The objective of this policy is to establish rules for the efficient and secure usage of email facilities and ensure that disruptions to the email facilities are minimized.

9.11 Human Resources Security Policy

The employees of NSEIT are its most critical assets and need to be protected accordingly. Also, the success of any information security initiative will depend on the support & participation of all employees & third-party personnel deployed at NSEIT. The objective of this policy is to ensure that all employees & third-party personnel working at NSEIT conduct themselves in a secure manner in compliance to the ISMS policies.

9.12 Information Sensitivity Policy

All the Information/ data accessed, processed and stored by NSEIT for its business processes (including customer provided data) need to be classified and marked in accordance with the Information Sensitivity policy.

The information / data will be classified into the following groups:

- Highly Confidential
- Confidential
- Internal Use
- Public Use

The Sensitivity Guidelines mentioned in the Information Sensitivity Procedures document provides details on how to protect information at varying sensitivity levels. The guidelines act as a reference only, as the NSEIT confidential information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the NSEIT confidential information in question.

9.13 Incident Management Policy

Any security related incident within NSEIT and/or related to NSEIT's business processes will be dealt by NSEIT's employees in accordance with the Incident management policy. The objective of this policy is to ensure that all security incidents are deal with in a quick and efficient manner, having the least impact on NSEIT's business processes.

9.14 License Management Policy

Only licensed software must be installed and used in NSEIT's business processes. The usage of software must confirm to the terms and conditions stipulated in the software's license document. The software licenses of NSEIT must be controlled by the system administrator of NSEIT. The objective of this policy is to control the unauthorized installation and proliferation of software owned by NSEIT.

9.15 Media Management & E-Waste Policy

The use of media for storage and movement of information should be strictly controlled in NSEIT. The usage of memory devices such as USB thumb-drives, flash memory devices, optical media etc must be subject to proper approval as given in the media management guidelines. The objective of this policy is to control the movement of information via means not directly under control of the ICT systems of NSEIT.
There is therefore a need to handle such disposals - referred to as E-Waste - in a responsible manner in line with emerging global best practices and standards.

9.16 IT E-Waste is a subset of E-waste and covers the following IT Equipment

S. No.	Category	Items
1.	Computers	Server/Desktop, Computer (CPU. Monitor, Keyboard and Mouse), Laptop, Notebook Dumb terminal etc. or similar items
2.	Printer & Accessories	Printer, Scanner, Printer Cartridge, Toner etc. or similar items
3.	Network Equipment's	Routers, Switches, Patch Panel, Modem, Converter, VSAT equipment's etc. or similar items
4.	IT Accessories	TV Tuner box, Floppy, CD and DVD, Pen Drive, External Hard disk, External CD / DVD writer, DAT Drive, Speaker, Laptop Battery, Hand Held device, VC equipment's, Data Cartridge, etc. or similar items
5.	Associated Electrical items	Power cable, Data cable, UPS, batteries, etc. or similar items

IT E-WASTE POLICY

The lifecycle of all IT assets spanning from acquisition to disposal shall be managed in a manner which conforms to sound environmental norms as detailed in the IT E-Waste guidelines. This includes:

- Preferential dealing with IT vendors having sound E-Waste management processes.
- Extending the useful life of IT assets to postpone / minimize generation of E - Waste
- Responsible disposal processes conforming to regulatory requirements and best practices.

IT E-WASTE MANAGEMENT GUIDELINES:

1. REGULATORY ENVIRONMENT

Different government bodies have published regulatory framework for handling E- waste. Similarly, different trade and industry bodies are also evolving the best. Practices to deal with IT E-Waste. CISO Office will scan the evolving code of practice and keep updating this policy document (supported by Corporate Steering Committee) in line with the best practices for disposal of IT E-Waste. This will be done once a year, or more frequently if deemed necessary.

The appropriate government bodies, e.g., Ministry of Environments & Forests/Central or State pollution control boards in India, etc. have initiated the process of approving and authorizing E-Waste Recyclers. CISO Office shall identify authorized. Recyclers, publish a list of such E-Waste Recyclers and enter into appropriate agreements covering all aspects of the E -Waste disposal.

2. IT E-WASTE MINIMIZATION PROCESS

- It shall be the endeavour of every user to maximize utilization of all IT assets to their full productive life. Apart from internal re-use, option to text end use outside NSEIT through donation to bonafide philanthropic institutions will also extend the useful life of IT assets.

- Only such IT assets which are non-operational and cannot be reused for any other alternate purpose should be considered as IT E-waste for disposal. The Asset Management team will certify this position.

3. COMPLIANCE REPORTING

As part of Quarterly IT Policy Compliance, the Asset Management team shall report the compliance to E-Waste Policy to the CISO, who in turn will present companywide consolidated status to the Corporate IT Steering Committee.

9.17 Network Administration Policy

The networks and communication services of NSEIT must be administered and controlled so to comply with the objective of the ISMS. The network must always serve its designated purpose without compromising the business requirements as well as the information security of NSEIT.

9.18 Password Policy

In order to safeguard information and computing resources from various environmental and other threats, a strong and effective password protection system should be mandated and implemented by NSEIT.
The objective is to protect them from unauthorized modification, disclosure or destruction and to ensure that information remains accurate, confidential and is available when required.

9.19 System Administration Policy

The information processing systems of NSEIT must be administered and controlled so to comply with the objective of the ISMS. The servers, desktops, printers and other such systems must always serve its designated purpose without compromising the business requirements as well as the information security of NSEIT.

9.20 Telecommuting Policy

Telecommuting refers to the situations where employee of NSEIT executes his/her official responsibilities from a location other than the usual official premises. The telecommuting privileges should be granted in a controlled manner so as to mitigate any information security risk arising from telecommuting.

9.21 Supplier Relationship Management

Supplier Management refers to manage suppliers and the services they supply, to provide seamless quality of IT service to the business, ensuring value for money be obtained.

9.22 Data Breach Management

The purpose of this policy is to provide a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to appropriate individuals and to outline the response to a confirmed theft, data breach or exposure based on the type of data involved.

9.23 Pandemic management

A pandemic is “an outbreak of a disease that occurs over a wide geographic area and affects an exceptionally high proportion of the population. ISO 27001 standard describes how to develop the Information Security Management System it defines that, first, NSEIT to find out which potential incidents might happen, and then define which kinds of safeguards NSEIT need to implement in order to prevent data breaches. So for employees who are working from home, NSEIT shall analyse which kinds of incidents can happen to the data stored on their computers and communicated over the Internet. Once this is done, only then NSEIT can decide whether employees will be required to use VPN, complex passwords, encrypt data, use only pre-approved cloud services, regularly back up the data, etc. Finally, accordingly shall document those rules through policies and procedures (Please refer BCP, System Administration and Network Administration policy documents)

10. Review and Maintenance

This policy will be subject to annual revision and, if revised, all employees will be alerted to the new version. Any queries on the security policy must be addressed to your department’s functional custodian.

The latest version can be found on the Sharepoint - NSEIT Quality Management System