ISMS Information Sensitivity Policy

RELEASE NOTICE

Document Name	ISMS Information Sensitivity Policy
Document Type	ISMS
Version	15.0
Release Date	14-Mar-2023
Document Number	ISMS/INFOSENPOL VER. 15.0

This document is subject to document control. Please keep it up to date using the release notices from the distributor of the document.

COPYRIGHT NOTICE

REVISION HISTORY

No.	Version	Preparedor Revisedby	Reason for Preparation or Revision	Review ed By	Approv ed By	Release Date
1	1.0	BS 7799 Implementation team	For use	CISO	CISO	22/07/2005
2	2.0	BS 7799 Implementation team	Incorporated changes as suggested by the BSI assessors	CISO	CISO	15/09/2005
3	3.0	ISO 27001 Implementation team	Incorporated changes as suggested by the BSI assessors	CISO	CISO	05/09/2006
4	4.0	ISO 27001 Implementation team	Incorporated changes to comply with ISO 27001	CISO	CISO	19/04/2007
5	5.0	ISO 27001 Implementation team	Incorporated changes to comply with ISO 27001	CISO	CISO	01/04/2008
6	6.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	15/09/2011
7	7.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	20/09/2012
8	8.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	23/09/2013
9	9.0	ISO 27001 Implementation team	Updated CISO Name	CISO	CISO	9/9/2014
10	10.0	ISO 27001 Implementation team	Incorporated changes to comply with ISO 27001:2013	CISO	CISO	23-July-2015

11	11.0	ISO 27001 Implementation team	Made changes in company logo, name, version and CISO name	S R Sharma	CISO	12-Aug-2016
12	12.0	ISO 27001 Implementation team	Company logo change	Mayuri Rachcha	CISO	24-July-2018
13	13.0	ISO 27001 Implementation team	Annual Review	Sheetal Gupta	CISO	28-April-2020
14	14.0	ISO 27001 Implementation team	Annual Review	Quality Team	CISO	02-Jan-2022
15	15.0	ISO 27001 Implementation team	Updated as per ISO 27001:2022 controls	CISO Team	CISO	14-Mar-2023

DOCUMENT APPROVAL

Name	Mr. Atul Shukla
Title	CISO
Signature	Mr. Atul Shukla
Date	14-Mar-2023

Table of Contents

1. Overview

NSEIT recognizes the need to protect data generated, accessed, modified, transmitted, stored or used in support of NSEIT's business processes. All employees of NSEIT have a responsibility to protect the organization's data in all formats, including electronic, physical, and/or intellectual. Classification of the data/information based on its sensitivity is essential to provide an adequate level of protection in terms of confidentiality, integrity and availability.

2. Purpose

The Information Sensitivity Policy is intended to help employees determine the sensitivityof information and govern its usage accordingly in terms of its access, storage, protection etc. This policy also provides 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.

This policy has been drafted by considering the requirements of the following ISO 27001:2022 controls:

A.5.12 Classification of information
A.5.13 Labelling of information
A.5.10 Acceptable use of information and other associated assets
A.8.3 Information access restriction
A.5.34 Privacy and protection of personally identifiable information

3. Scope

This policy applies to all data generated, accessed, modified, transmitted, stored and/or usedby the employees of NSEIT irrespective of the medium on which it resides and regardless of format. This includes electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

Queries regarding these guidelines and on proper classification of a specific piece of information should be addressed to the concerned department's functional custodian.

4. Convention

Steps prescribed for the reader in this policy are mandatory except when preceded by the word "may". The term hardcopy is used to denote all information in paper format such as printouts, postal mail records etc. and the term softcopy is used to denote information in electronic format such as software source code, websites, email records etc.

5. Abbreviations and Acronyms

TABLE 5.1 – ABBREVIATIONS AND ACRONYMS

Acronym& Abbreviations	Full Form
NSEIL	National Stock Exchange of India Limited
NSEIT	Technology subsidiary of the NSEIL
ISMS	Information Security Management System

6. Policy

The information sensitivity policy classifies information of NSEIT into the following four categories:

- NSEIT Public
- NSEIT Internal Use
- NSEIT Confidential
- NSEIT Highly Confidential

The classification has been defined based on the access restrictions that need to be imposed depending on sensitivity of information and the "need-to-know" of end user. The access control matrix defined for NSEIT's information assets is given below:

Classification of Information	Access at Individual Level	Access at Departmental Level	Access at Organizational Level
NSEIT Public (Information such as corporate website, product brochures, press clippings)	Access to all employees, third party personnel & outside world	Access to all employees, third party personnel & outside world	Access to all employees, third party personnel & outside world
NSEIT Internal Use (E.g. Information such as corporate intranet, newsletters, ISMS policies)	Access to all employees & third-party personnel	Access to all employees & third- party personnel	Access to all employees & third party personnel

NSEIT Confidential (E.g. Software source code, NIPM documentation, proposals & contracts)	Access to all employees of department handling the information asset, unless specific audience is mentioned	Access to all employees of department handling the information asset, unless specific audience is mentioned	Access is Restricted
NSEIT Highly Confidential (E.g. Personnel information such as salary slips & records on background verifications, Business critical information such as Board of directors' minutes of meetings, business strategy related documents)	Access to employees specifically mentioned as audience	Access is Restricted	Access is Restricted

7. Information Labelling and Classification Guidelines

The Information Labelling & Classification Guidelines below provide details on how to protect information based on their sensitivity. These guidelines should be treated as mandatory for all information belonging to NSEIT.

Certain information may necessitate more stringent measures of protection over and above those given in the guidelines, depending upon the circumstances and the nature of the information in question. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their functional custodian for further clarity.

7.1 NSEIT Public

NSEIT Public information is information that has been declared public knowledge by senior management and can freely be given to anyone without causing any possible damage to NSEIT Ltd.

Labelling	Labelling is at the discretion of the owner or custodian of the information. If labelling is desired, the words " NSEIT Public" may be written or designated in a conspicuous place on or in the information inquestion. All information without a label will be treated as "NSEIT Public" information.
Access	NSEIT employees, third party personnel & outside world.
Distribution within NSEIT	Standard interoffice mail, approved electronic mail and electronic file transmission methods such as ftp.

Distribution outside of NSEIT	Indian postal mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Storage	Hardcopies of such information may be stored anywhere in NSEIT premises subject to maintaining "clear desk" policy and other office discipline. Softcopies of such information such as corporate website etc may be stored in any desktop / server of NSEIT.
Disposal/Destruction	Hardcopies should be shredded and disposed of within NSEIT premises. Softcopies should be deleted from respective locations.
Penalty for deliberate or inadvertent disclosure	None, however, any unauthorized modifications / deletion of such information which may adversely affect NSEIT will be treated as a security incident and taken up accordingly.

7.2 NSEIT Internal Use

NSEIT Internal Use is information whose access & use is restricted to only employees & third-party personnel working at NSEIT. This classification will not extend to sensitive information whose disclosure to the outside world may adversely affect NSEIT's business prospects. NSEIT Internal Use is typically information that has no "Intellectual Property" value but is needed for efficient & secure operations of NSEIT.

Labelling	"NSEIT Internal Use" should be written or designated in a conspicuous place on or in the information in question.
Access	NSEIT employees and third-party personnel who have a business need to know
Distribution within NSEIT	standard interoffice mail, approved electronic mail and electronic file transmission methods such as ftp.
Distribution outside of NSEIT	Subject to approval from immediate manager. Once approved, the information may be sent using Indian postal mail and other public or private carriers, approved electronic mail and electronic file transmission methods

Storage	Such information should be stored only in machines designed for access throughout organization. Copies of the same may be maintained by individual employees. However, the same must be marked as "Uncontrolled Copy" whether in electronic or paper format and it is the employee's responsibility to ensure that the information is not divulged to the outside world.
Disposal/Destruction	Hardcopies of information should be shredded and disposed within NSEIT premises. Softcopies should be deleted from respective locations.
Penalty for deliberate orinadvertent Disclosure	Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law

7.3 NSEIT Confidential

NSEIT Confidential is information whose access & use is restricted to all employees of select departments or to select employees of select departments of NSEIT. Such information may include intellectual property of NSEIT such as software source code, proposals, audit reports etc, which on disclosure to the outside world may adversely affect the business prospects of NSEIT.

Labelling	"NSEIT Confidential" should be written or designated in a conspicuous place on or in the information in question
Access	NSEIT employees and third party personnel designated with approved access and having signed non-disclosure agreements. The access privileges should be defined as multiple levels such as Read+Write+Copy, Read+Write or Read only access and only the minimum privileges required to execute concerned business processes should be granted to employees. Unless specified, the access privilege shall be "Read Only". Access rights of such information are not automatically transferred to derived or referenced information.

Distribution within NSEIT	Hardcopies should be delivered in sealed envelopes stamped confidential. Softcopies should be delivered via corporate email system or approved information transfer methods such as VSS servers, SVN Servers, ftp connections etc.
Distribution outside of NSEIT	Hardcopies should be delivered in sealed envelopes marked confidential and carried by only approved personnel or approved private carriers and the signature of recipient should be obtained. This procedure is also applicable to information sent on media such as LTO tapes, Cloud with most secured encryption.
Storage	Hardcopies should be stored in locked cabinets & drawers within NSEIT premises, with strict control over access to the cabinet/drawers keys.
	Softcopies should be stored in desktops of authorized employees or in servers designated for the same Encryption may be used to further secure the information, provided accesses to encryption keys are restricted to the information owner or custodian.
Disposal/Destruction	Hard copies to be disposed of should be placed in collection binsdesignated for shredding. The copies may be manually torn prior to disposing the same in the collection bin. Soft copies should be deleted from all storage locations and the same should be formatted & is possible.
Penalty for deliberate or inadvertent disclosure	Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

7.4 NSEIT Highly Confidential

NSEIT Highly Confidential is information whose access & use is restricted to only employees specifically authorized by senior management of NSEIT. Such information has highest sensitivity with respect to NSEIT's business processes and include information such as minutes of meetings of Board of Directors, Documents related to business strategies of NSEIT etc. Disclosure of such information would result in loss of business as well as a host of legal complications for NSEIT.

Labelling	"NSEIT Highly Confidential" should be written or designated in a conspicuous place on or in the information in question. The labelling should also be embedded as a watermark on all pages of such information.

Access	NSEIT employees who have been specifically authorised by senior management of NSEIT. The access privileges should be defined as multiple levels such as Read+Write+Copy, Read+Write or Read only access and only the minimum privileges required to execute concerned business processes should be granted to employees. Access may also be defined for a specific duration of time. Access rights of such information are not automatically transferred to derived or referenced information.
Distribution within NSEIT	Hardcopies should be in sealed envelopes stamped Highly Confidential and hand delivered by authorized NSEIT employee and signature of recipient should be obtained. Softcopies should be delivered via corporate email system after due encryption of the same.
Distribution outside of NSEIT	Hardcopies should be in sealed envelopes stamped Highly Confidential and hand delivered by authorized NSEIT employee and signature of recipient should be obtained. This procedure is also applicable to information sent on portable media such as flash drives, CD/DVD-ROMS. Softcopies should be sent in an encrypted format with approved means of transmitting the encryption keys.
Storage	Hardcopies should be stored in fireproof safes within NSEIT premises, with strict control over access to the safe keys. The access to safes should be logged restricted to select authorized employees. Whenever possible, the hardcopy should be in green color paper to deter attempts of photocopying. Softcopies should be stored in desktops of senior management or authorized employees in an encrypted format. A copy of the encryption key should be available with senior management.
Disposal/Destruction	Hardcopies to be disposed should be personal shredded by information owner using the shredded machine. Softcopies should be deleted from storage media and the sameshould be sanitized if possible.
Penalty for deliberate or inadvertent disclosure	Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

8. Enforcement

Any employee or third-party personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9. Review and Maintenance

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

END OF POLICY