|  |
| --- |
| NST LOGO.jpg |
| **Document & Record Management Procedure** |
|  |
|  |
|  |
|  |

**Version History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver.** | **Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 16th Oct 2013 | Initial draft | Rahul Raj | Dhananjay Kumar | Ajay Kumar Zalpuri |
| 1.0 | 30th Sep 2013 | Initial release | Rahul Raj | Dhananjay Kumar | Ajay Kumar Zalpuri |

**Table of Contents**

[1. Purpose 4](#_Toc369779203)

[2. Preparation of ISMS Documents 4](#_Toc369779204)

[3. Document Control Features 4](#_Toc369779205)

[4. Revisions 4](#_Toc369779206)

[5. Security of Documents 5](#_Toc369779207)

[6. Control of Records 5](#_Toc369779208)

# Purpose

The purpose of the procedure is to develop and manage the system to ensure the control, maintenance and archive of quality records.

It is applicable for preparation, approval, issue, revision, distribution and destruction of: -

- Information Security Management System Manual

- Information Security Management System Policies, Procedures and other relevant documentation

# Preparation of ISMS Documents

MR shall issue the Latest version of all the ISMS related documents (process, procedure, guidelines, templates and checklists).

* 1. Information Security Management System Manual
     1. ISMS Manual will be prepared by Chief Information Security Officer (CISO) and approved by Sponsor
  2. Information Security Management System Policies
     1. Sponsor shall establish the ISMS in consent with CISO.
  3. Information Security Management System Process, Procedure, templates and form
     1. Respective functional head shall develop the ISMS processes and procedures with the help of MR and approved by CISO

# Document Control Features

* 1. Dissemination of Documents
     1. Dissemination of documents of ISMS shall be done by MR. It will be uploaded in TFS server/Intranet. The documents shall be in read-only mode with proper authentication for access.

* 1. Uploading of Documents on TFS server/Intranet
     1. MR are responsible for hosting of Procedures/ Instructions / Policies on the TFS server/ Intranet, after due approval from the competent authority.
  2. Documentation Access Rights
     1. All ISMS documents are available on TFS server/Intranet only for viewing purpose.

Access right (Read/write/delete) for each role shall be maintained in Process Asset library.

* 1. Master List of Documents
     1. MR shall maintain the master list of ISMS documents as Process Asset Library on TFS server/Intranet

# Revisions

* 1. Information of Document Revisions
     1. MR shall intimate about the revision of the concerned documents to authorized personnel through email as and when required.
  2. Control features for revisions
     1. Nature of revisions from the earlier version shall be recorded in the revision history of document itself.
     2. Before uploading the revisions, the MR shall update the Process asset library.
  3. Obsolete documents
     1. All obsolete documents may be maintained in archive folder for future reference and knowledge purpose.

# Security of Documents

* 1. Security

Security aspects cover the steps to be taken against tampering of documents intentionally or by a system crash due to any reason. IT Manager shall be responsible for security aspect of these documents.

1. Taking back-up monthly.
2. Taking back-up of files as and when changes are made to the documents.
3. To keep a backup in the offsite storage, wherever required.
4. To Maintain records of such backups
5. Access to documents given only to authorized persons
6. Only authorized persons use the information.

# Control of Records

* 1. Records are maintained as hard copies or soft copies or both as per requirements
  2. Quality Records, their retention period, location and the person responsible for their control, retention and its nature i.e. whether maintained as softcopy / hardcopy /Both are identified and defined in ISMS Manual.
  3. Similarly in case, softcopy of these records are maintained, the corresponding directory path is specified instead of location along with rest of details. For soft copies, which require security, they will be part of a secured directory structure in the form of read only copies.
  4. The person responsible to maintain and control Quality Records is also responsible for their review to maintain effectiveness of the ISMS.
  5. All Quality Records are indexed identifying type / nature of the record / year / period.
  6. All Quality Records whether in the form of Hard copies or Soft copies are stored and retained to ensure they are easy and readily accessible/retrievable, whenever required, and to prevent damage/loss.
  7. All Quality Records are retained for a defined period or required to fulfill the contractual obligation/ agreement, whichever is later. Obsolete records, which need not to be retained after their retention period, are disposed off considering nature of the record and after seeking approval from CISO.
  8. Accordingly, once in a year, such dispositions are planned under CISO’s knowledge/approval.
  9. All Department Heads / MR ensure that the Quality Records are made available to the customer, where this is an agreed contractual requirement and the external/ internal auditors at the time of quality audits.
  10. Quality Records required to be retained for legal / knowledge purpose are preserved for a period, more than the defined retention period, are identified and kept separately.
  11. All the persons, responsible to maintain Quality Records, related to their areas / functions.
  12. MR maintains the Master List of Quality Records.