North Shore Technologies

Information Security Management System

(ISMS) Manual

Version History

Ver.	Date	Description of Change	Authored / Revised By	Reviewed By	Approved By
0.1	16-Aug 2013	Initial draft	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
1.0	31st Oct 2013	Initial Release	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
1.1	3rd Dec 2013	Reviewed & hyperlink the process	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
1.2	15th Sep 2014	Update in control A.11.1.3 for physical access control for Biometric and CCTV Monitoring. Update in control A.9.1.2. for access to network and network services by binding IP address through MAC	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.0	29th June 2015	Modify Clauses, section & controls to meet the requirements for new version of ISMS 27001:2013 and update HR responsibilities.	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.1	27th May 2016	Update in control A.9.3.1, A.9.1.1, A.13.1.1 for Migration to cloud services. ISMS awareness training through induction included in control A.7.2.2	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.2	3rd May 2017	Modify section 4.2 Understanding the Needs and Expectation from Interested Parties for external/vendor. Update section A.17.2.1 for redundancy buildup through IT operation process for firewall changes for HA	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.3	5th Feb 2018	Update in control A.7.1.1 and A.7.3.1 for HR policies update like background verification, Exit policy and No code sharing policy. Update in control A.13.2.4 for Project specific NDA. Update section Key Objective 1 for On time delivery and increase threshold value from 80% to 90%	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.4	3rd Dec 2018	Update in control A.9.3.1 for O365 (Multifactor Authentication and Single sign-on and update in password policy for VPN for complex password. Update in control A.12.2.1 for antivirus policy using Bit Defender instead of MacAfee	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.5	4th March 2019	Update in control A.15.2.1 for changes in procurement process for SAP usage, online purchase and purchase directly through OEM. Update in control A.11.2.7 and A.8.3.2 for E-waste Disposal. Update in control A.13.1.3 for Increase in Subnet for more effective communication. Update in control A.7.2.2 for increasing ISMS Awareness through online assessment. And section 5.3 for roles & responsibility	Rahul Raj	Dhananjay Kumar	Ajay Kumar Zalpuri
2.6	14th April 2020	Update section 5.3 Role & Responsibility for New MD and CSO. Add HR and Security Officer	Rahul Raj	Dhananjay Kumar	Nand Kishore

Table of Contents

ABBREVIATION

ABBREVIATION	DESCRIPTION
BCP	Business Continuity Plan
CIA	Confidentiality, Integrity and Availability
CISO, NST (P) LTD.	Chief Information Security Officer
DB	Database
DP	Departmental Procedure
DR	Disaster Recovery
DRO/HOF	Direct Reporting Officer / Head of Function to Head of
ED	Executive Director
HOD	Head of Department
HQ	Head Quarter viz., NST (P) LTD.
HR	Human Resource
HRDC	Human Resource Development Center
HRDD	Human Resource Development Department
HRDI	Human Resource Development Institute
IPR	Intellectual Property Right
IS	Information Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISSC	Information System Security Committee
ISSO	Information System Security Officer
IT	Information Technology
NC	Non-Conformity
NDA	Non-Disclosure Agreement
OEM	Original Equipment Manufacturer
RA	Risk Assessment
RTP	Risk Treatment Plan
SOA	Statement of Applicability
SP	Standard Procedures
TSX	Technical Services Department
VA	Vulnerability Assessment

1 Introduction

This section presents the Scope of the Information Security Management System (ISMS). This includes the purpose and the application of ISMS.

1.0 Scope

The Scope of the ISMS covers, the North Shore (P) Ltd, its Server room and its management related to business applications, to implement the IT services provided to internal and external customers from its office location at Logix Techno Park, Sector-127, Noida.

(Note: refer to Latest version of '**NST-ISO27001-2013-SOA-V2.1.xlsx'** for exclusions)

1.1 General

This ISMS manual specifies the requirements for establishing, implementing, monitoring, reviewing, maintaining, and improving documented ISMS within the context of the overall Business requirements. It specifies the implementation of security controls customized to the needs of NST (P) Ltd.

The ISMS is designed to ensure adequate and appropriate security controls that maintain Confidentiality, Integrity and Availability (CIA) of information assets.

For applicability (with rationale) and exclusion (with justification) of controls refer Statement of Applicability (SOA). The SOA as applicable to NST (P) Ltd is enclosed. As certain controls are not applicable at project sites, project site specific SOA is also made.

1.2 References

The following documents were referred for the creation of this document. These include:

- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

1.3 Terms and Definitions

- **Asset** – Anything that has a value to the organization.

- **Availability** – The property of being accessible and useable upon demand by an authorized entity.

- **Business Continuity Plan (BCP)** – A plan to build-in proper redundancies and avoid contingencies to ensure continuity of Business.

- **Computer Media** – Includes all devices that can electronically store information. This includes but not limited to diskettes, CD's, tapes, cartridges, and portable hard disks.

- **Confidentiality** – Ensuring that information is accessible only to those authorized to have access.

- **Continual Improvement** – Continual Improvement refers to stage improvement programs that facilitate rapid improvement phases with intermediate stabilized phases.

- **Control** – A mechanism or procedure implemented to satisfy a control objective

- **Control Objective** – A statement of intent with respect to a domain over some aspects of an organization's resources or processes. In terms of a management system, control objectives provide a framework for developing a strategy for fulfilling a set of security requirements.

- **Disaster Recovery (DR)** - A plan for the early recovery of Business operations in the event of an incident that prevents normal operation.

- **Fallback** – Provisions to provide service in the event of failure of computing or communications facilities.

- **Information Security** – Security preservation of Confidentiality, Integrity and Availability of Information.

- **Information 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 involved.

- **Information Security Incident** – A single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

- **Information Security Management System (ISMS)** – That part of overall management system based on 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.

- **Integrity** – Safeguarding the accuracy and completeness of information and processing methods.

- **Organization** – Refers to NST (P) Ltd unless specified otherwise.

- **Risk** – The combination of the probability of an event and its consequence.

- **Residual Risk** – The risk remaining after risk treatment.

- **Risk Acceptance** – Decision to accept risk.

- **Risk Analysis** – Systematic use of information to identify sources and to estimate the risk.

- **Risk Assessment** – Overall process of risk analysis and risk evaluation.

- **Risk Evaluation** – Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

- **Risk Management** – Coordinated activities to direct and control an organization with regard to risk.

- **Risk Treatment** – Process of selection and implementation of measures to modify risk.

- **Statement of Applicability –** Document describing the control objectives and controls that are relevant and applicable to NST (P) Ltd ISMS, based on the results and conclusions of the Risk Assessment and Risk Treatment Processes. It should clearly indicate exclusions with appropriate reasons.

2 About the Manual

This section presents a brief overview of the Information Security Management System (ISMS) manual of NST (P) Ltd.

2.1 Organization of the Manual

The ISMS manual is intended as a reference document describing the security framework adopted by NST (P) Ltd. It is organized as per the Table of Contents.

2.2 Document Availability

This document is available to all employees of the NST (P) Ltd in the form of web page on the intranet. This is a read-only copy and the relevant part of the documentation is available to only authorized users based on their business requirements.

2.3 Document Control Information

It is the responsibility of the NST (P) Ltd to release an approved document for the NST (P) Ltd.

3 Organization Overview

This section presents an overview of the NST (P) Ltd and its operations.

NST mission is to fulfill the promise of applying technology to enable the success of customer business by performing at a level of trust, partnership, and innovation that far exceed what you have come to expect from technology services providers. In the same way, we know that to achieve that aspiration, we must exceed what our professionals have come to expect from technology services employers.

4 Context of the Organization

4.1 Understanding the Organization and it’s Context

NST shall determine external and internal issues that are relevant for delivering the services from Server Room and Business Operation that affect its ability to achieve the intended results of ISMS. The issues which are considered necessary for delivering the services to internal and external stakeholders are given in the table after section 4.2.

4.2 Understanding the Needs and Expectation from Interested Parties

NST shall determine the following:

a) Interested parties that are relevant to ISMS - All customers (Internal and External), Vendors, Supporting the Infrastructure in Server Room & other Business operation, all employees providing & getting services to Server Room & other Business operation.

b) The requirement of these interested parties relevant to Information Security The needs and expectations from external as well as internal customers are considered as under and will be reviewed and updated over a period of time as part of continual improvement.

	Stake holders	Issues

Internal	Management	Governance, Resource availability, organization structure, roles and accountabilities, Policies, objectives, and the strategies
	Employees	Fulfillment of commitments, adherence to organization policies, processes and guidelines and to ensure seamless / uninterrupted operations. Expectation of employees in terms of commitment made by the organization need to be fulfilled.
	Shareholders	Relationship with, and perceptions and values of, internal stakeholder's
	Board of Directors	Maintaining commitment to customers, goodwill and repute of the organization, and maintaining return on investment committed on the business, in totality
	Corporate requirements	Standards, guidelines and models adopted by the organization
	Users / Other departments	Information technology related requirements to the organization such as access right, IT infra availability to internal users and other departments.
	HR	Resource availability, resource competence, training, background verification etc.,
	Finance	Approval of financial commitments
	Legal	Vetting of Legal contracts and protecting the organization from non-compliance of legal, regulatory and contractual requirements

External	**Customers**	**Service delivery**
	Vendors	Supply of goods and services to enable the organization to meet the requirement of the customer. Compliance with relevant legal, statutory and contractual requirements.
	Users / Public	Information technology related requirements to the organization such as access right, IT infra availability to internal users and other departments.
	Government	Submission of desired reports and statements and approvals to carry out the business. Fulfilling the legal, and regulatory requirement.
	Society and environment	Natural and competitive environment, Key drives and trends having impact on the objectives of the organization, Political, financial status of the country.

4.3 Determining the scope of the Information security management System

The Scope of the ISMS covers,

- The NST Server Room, Business Operation and its management
- To implement the IT services provided to internal and external customers

Server room is located at North Shore Technologies Pvt. Ltd, 1st Floor, Tower-B, Logix Techno Park, Sector-127 | Noida

(Note: refer to SOA for exclusions)

Information Security Management System

NST shall establish, implement, Maintained and continually improve an information security management system, in accordance with the requirements of ISO 27001:2013.

5 Leadership

This section presents the NST (P) LTD.'s initiative and commitment to effective implementation and operation of ISMS. In addition, this section highlights the roles and responsibilities associated with ISMS operation.

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information Security management system by:

a. Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
b. Ensuring the integration of the information security management system requirements into the organization's processes;
c. Ensuring that the resources needed for the information security management system are available;
d. Communicating the importance of effective information security management and of conforming to the information security management system requirements;
e. Ensuring that the information security management system achieves its intended outcome(s);
f. Directing and supporting persons to contribute to the effectiveness of the information security management system;
g. Promoting continual improvement; and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5.2 ISMS Policy

NST is committed to maintain **high quality standards** in **delivering timely** and **cost effective** solutions to our customers by **continual improvement** of our processes, instilling **quality consciousness** amongst all employees and recognizing the **confidentiality, integrity** and **availability** of information assets to relevant stakeholders including our customers.

Risk management will be done as per NST-CP-05-ISMS-RART-Risk Assessment & Risk Treatment Procedure and the risk will be evaluated based on asset value, threat and vulnerabilities. If risk value is high, adequate controls will be implemented.

Action Guideline:

i. NST (P) Ltd prevents leakage, destruction, and illegal use of all information relating to the customers, vendors, management etc. and builds the system to secure the confidentiality, integrity and availability of the information for daily operations.

ii. Company recognizes the value of the private information of all staff and secures it.

iii. NST (P) Ltd establishes a contingency plan to secure continuation of the business, assuming occurrences of a natural disaster, terrorism, a large-scale infection disease etc.

iv. Company provides all staff with proper education and training to maintain and improve the effectiveness of the information security management system

v. Company builds and manages an organization which grasps incidents, audits its operations and effectiveness of the information security management system, and attempts its continuous improvement.

To secure its information assets and its customer, NST shall deploy procedures to maintain confidentiality, integrity and availability of all information assets

Business objectives and goals of NST are

1. **Key Objective 1:** Provide high quality services to our clients.
   Goal 1 – Client Satisfaction Score of more than 90 %
   Goal 2 – On time Delivery >90%
   Goal 3 – No defects of showstopper/critical type in first release to the client.

2. **Key Objective 2:** Continuous focus on employee satisfaction and competency development so as to reduce and stabilize employee attrition.
   Goal 1 – A minimum of 4-man days training in a year per employee.
   Goal 2 – Overall attrition rate <15% in year
   Goal 3 – Employee satisfaction survey score of greater than 75%

3. **Key Objective 3:** Continual improvement of services to our internal & external customers.
   Goal 1 – Key process performance improvement of at least 10% per annum in all departments

4. **Key Objective 4:** To secure its information assets and of its customers, NST shall deploy procedures to maintain confidentiality, integrity and availability of all information assets.
   Goal 1 – Number of security incidents of high severity to be less than 5% of total security incidents.

5. **Key Objective 5:** To have year on year revenue increase while maintaining profitability
   Goal 1 – Revenue growth of >=40% with respect to the previous financial year
   Goal 2 - Profit before Tax to be >=20%

To meet these business goals, ISMS objective are defined. Which are given in section 6.2

5.3 Organizational Roles, Responsibilities & Authority for Information Security

NST (P) LTD. is committed to security. The management has constituted Information System Security Committee, which is responsible for defining and improving the ISMS.

Management provides evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS as defined in ISMS documentation, by

a) Establishing an information security policy;
b) Ensuring that information security objectives and plans are established;
c) Establishing roles and responsibilities for information security;
d) Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
e) Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS;
f) Deciding the criteria for accepting risks and the acceptable level of risk;
g) Ensuring that internal ISMS audits are conducted;
h) Conducting management reviews of the ISMS.

SPONSOR (Nand Kishore Avantsa)

- Establishing an ISMS policy & integrated quality policy
- Ensuring that ISMS objectives and plans are established.
- Establishing roles and responsibilities for information security.
- Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement:
- Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS.
- Deciding the criteria for accepting risks and the acceptable levels of risk.
- Ensuring that internal ISMS audits are conducted
- Conducting security Committee meetings of the ISMS

CHIEF INFORMATION SECURITY OFFICER- NST- (Manish Sehgal)

- Responsible for defining ISMS Framework.
- Responsible for implementing ISMS Framework
- Responsible for Publishing ISMS Manual
- Responsible for ensuring that security incidents are handled and resolved in efficient manner.
- Define specific roles and responsibilities of information security across the NST (P) LTD.

INFORMATION SYSTEM SECURITY COMMITTEE (SEPG WILL TAKE CARE)

- Develop, maintain, and implement ISMS policies and procedures
- Develop and maintain Business Continuity Management Plan for the region.
- Approve and review the risk treatment plan, and accept residual risk
- Design and deliver awareness program
- Evaluate, implement and ensure utilization of up-to-date security technology and techniques
- Review and monitor information security incidents
- Ensure ISMS is in line with new legal, administrative, and business requirements
- Ensures that security is part of the information planning process
- Decide specific methodologies and processes for information security. For e.g. risk assessment, security classification system etc.
- Drive NST (P) LTD. wide information security initiative

- Assess new system and services for security before absorbing them into the system and identify and implement appropriate security controls

MANAGEMENT REPRESENTATIVE (RAHUL RAJ)

- Responsible for defining policies and processes
- Responsible for owning the security policy and reviewing and evaluating the same at least once in a year.
- Responsible for reviewing current implementation of policies and processes and improving them if required
- Responsible for reviewing security incidents and vulnerabilities and decide action to be taken on them
- Responsible for reviewing any kind of hacking attacks and action taken to control them
- Reviewing security audit reports and action taken to resolve NCs
- Reviewing disciplinary action taken against employee (if there is any such case)
- Review Backup audit reports and action taken on them.
- Member of Information system Security Committee.
- Co-ordinates with Information System Security Committee.
- Organize security reviews and audits, with internal and external resources
- Ensure implementation and tracking of ISMS plan
- Organize management reviews of ISMS
- To promote awareness amongst employees on ISMS.

MANAGER IT (SAKET MADAN)

- Heading NST (P) Ltd, IT
- Heading IT processes
- Follow up daily tasks and tickets
- Handling system security incidents and vulnerabilities
- Handling virus attacks and hacking attacks and reporting them to Security Committee
- Responsible for reviewing current implementation of policies and processes and improving them if required
- Responsible for reviewing any kind of hacking attacks and action taken to control them
- Reviewing security audit reports and action taken to resolve NCs
- Reviewing disciplinary action taken against employee (if there is any such case)
- Review Backup audit reports and take action on it
- Member of Security Committee
- Managing IT resources
- To review and prioritize significant information Assets and security threats
- Incidents Reporting

HR MANAGER (AMITA SHITAL)

- Heading HR Processes
- Follow up daily tasks and HR Issues
- Handling employee related incidents (misconducts, policy violations and other offences) and taking appropriate action against employees if required and reporting them to security Committee.

- Take care of Human resource security clauses prior to employment, during employment and Termination or change of employment.

PMO

- Resource Management
- Onboarding/Exit
- Project Administration
- Timesheet Management
- Technical Training

ADMIN ASSISTANT MANAGER (BHUPESH KAKKAR)

- Heading Admin Processes
- Follow up daily tasks and Admin Issues
- Handling employee related admin issue (misconducts, policy violations and other offences) and taking appropriate action against employees if required and reporting them to security Committee
- Managing Admin resources
- Physical Security and Physical Access Control

MANAGER IT NETWORKS (SAKET MADAN)

- Planning and monitoring networks
- Handling network issues
- Network setup and management
- Reviewing server logs (which includes operator and administrator logs)
- Client servers Monitoring support
- Antivirus support
- Handling network security incidents
- Handling virus attacks and hacking attacks and reporting them to Information System Security Committee
- Managing Network resources

SYSTEM ADMINISTRATOR (SAKET MADAN)

- Ticket assignment
- Ticket escalations from engineers
- IMS Management
- Data Backups
- Server usage tracking
- Helpdesk
- Reports Management

NETWORK ENGINEER (IT SUPPORTS TEAM)

- Ticket assignment, Ticket Handling
- Desktop Issues
- Maintaining Spare Parts details
- Maintaining Software upgrade
- Operating System patch management

VENDORS

- Provide services as per defined SLA
- Provide Technical Support
- Provide resources for upkeep of Data Center

USERS

- Will follow the ISMS Policies
- Will not share passwords
- Will use application as per the scopes and access provided
- Will maintain assets in good condition

The Security Committee will meet once every month, support and supervise the activities of the NST (P) LTD., taking informed decisions. It will be held responsible for achieving measurable progress. Process measurement metrics will be monitored to achieve continuous improvement.

Risk Assessment and BCP CORE TEAM (Sudhir, Dhananjay, Saket and Rahul)

Review, test and reassess the strategy plan to determine the overall approach to business continuity. Responsible for reviewing security incidents and vulnerabilities and decide action to be taken on them

- Identify and define plans to protect critical business process from the major failure of information system or disasters and to ensure timely resumptions of business activity
- Review, test and reassess the strategy plan to determine the overall approach to business continuity.
- Responsible for reviewing security incidents and vulnerabilities and decide action to be taken on them
- Carry out RA and prepare RTP

Note: - Any two of the four members are mandatory to carry out this activity.

In addition, the group helps reduce the risk of disruption of business operation by providing advice on all aspects of security including:

- Security Awareness
- Data Confidentiality and Privacy
- Logical Access
- Data Communications
- Systems and Data Integrity
- Physical Security
- Personal and Procedural Controls
- Contingency and Disaster Recovery Planning

EMPLOYEES

Expected to follow security policy, processes, and procedures as documented in ISMS.

5.3.1 Security Domains addressed by ISMS

Following are the domains being addressed by ISMS:

- **Security Policy (A.5):** Management direction and support for IS in accordance with business requirements and relevant laws and regulations.
- **Organization of Information Security (A.6):** Maintain security of information within the organization and its processing facilities that are accessed, processed, communicated to, or managed by external parties.
- **Human Resources Security (A.7):** Clear roles and responsibilities, IS awareness and trainings, exiting the organization in an orderly manner.
- **Asset Management (A.8):** To appropriately classify and protect the organizational assets.
- **Access Control (A.9):** Prevent unauthorized access to information systems, networked services, operating systems, application systems, and ensure IS when using mobile computing and teleworking facilities.
- **Cryptography (A10) deals with cryptographic controls.**
- **Physical and Environmental Security (A.11):** Preventing unauthorized physical access in the premises and loss/damage/theft of equipment's.
- **Operational security (A12)** Ensuring secured networks, maintaining appropriate third-party service delivery agreements, minimize risk of systems failures, and protect software and information integrity.
- Communication Security (A13) Deals with Network communication, Information transfer and communication with suppliers.
- **Systems Acquisition, Development and Maintenance (A.14)**: Prevent errors, loss, unauthorized modification or misuse of information in applications, ensure security of system files and software, and reduce risks resulting from exploitation of published technical vulnerabilities.
- **Supplier Relationship (A.15) Information security in supplier relationship and supplier agreements**
- **Information Security Incident Management (A.16):** Timely communication of IS events and weaknesses and taking corrective actions.
- **Information Security aspects in Business Continuity Management (A.17):** Counteract interruptions to business and protect critical business processes from effects of major failures or disaster, and to ensure timely resumption

- **Compliance (A.18):** Complying with legal requirements, security policy and standards.

6 Planning

6.1 Actions to address risks and opportunities

6.1.1 General

When planning for the information security management system, NST shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

a) Ensure the information security management system can achieve its intended outcome(s);
b) Prevent, or reduce, undesired effects; and
c) Achieve continual improvement.

NST shall plan:

d) Actions to address these risks and opportunities; and
e) How to
   1. Integrate and implement the actions into its information security management system processes; and
   2. Evaluate the effectiveness of these actions.

6.1.2 Information security risk assessment

NST shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria that include:
   1. the risk acceptance criteria; and
   2. criteria for performing information security risk assessments;
b) ensures that repeated information security risk assessments produce consistent, valid and comparable results;
c) identifies the information security risks:
   1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
   2. identify the risk owners;
d) analyses the information security risks:
   1. assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
   2. assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
   3. determine the levels of risk;
e) evaluates the information security risks:
   1. compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
   2. Prioritize the analyzed risks for risk treatment.

NST shall retain documented information about the information security risk assessment process.

6.1.3 Information security risk treatment

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

a) select appropriate information security risk treatment options, taking account of the risk assessment results;
b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE: NST can design controls as required or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A of the standard ISO 27001:2013 and verify that no necessary controls have been omitted;

NOTE 1 Annex A of the standard ISO 27001:2013 contains a comprehensive list of control objectives and controls. Users of this International Standard are directed to Annex A of the standard ISO 27001:2013 to ensure that no necessary controls are overlooked.

NOTE 2 Control objectives are implicitly included in the controls chosen. The control objectives and controls listed in Annex A of the standard ISO 27001:2013 are not exhaustive and additional control objectives and controls may be needed.

d) Produce a Statement of Applicability that contains the necessary controls (see 6.1.3 b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
e) Formulate an information security risk treatment plan; and
f) Obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks. The organization shall retain documented information about the information security risk treatment process.

The details of the RA process can be referred from **'PROCEDURE FOR RISK ASSESSMENT AND TREATMENT'**

The outputs of the RA process include:

- Risk Assessment Report
- Risk Treatment Plan
- Statement of Applicability (inclusion with rationale /exclusion with justification)

Based on the RA report, Information System Security Council prepares the RTP, which includes selection of controls. The NST then obtains management approval for RTP implementation and acceptance of residual risk.

6.2 Information security objectives and planning to achieve them

NST. Shall establish information security objectives at relevant functions and levels. The information security objectives shall:

- be consistent with the information security policy;
- be measurable (if practicable);

- take into account applicable information security requirements, and results from risk assessment and risk treatment;
- be communicated; and
- Be updated as appropriate.

NST shall retain documented information on the information security objectives.

Following are the ISMS Objectives established by senior management:

ISMS Objectives

i. Protect information from deliberate or unintentional unauthorized acquisition or unauthorized access

ii. Maintain confidentiality of information

iii. Maintain integrity of information by protecting it from unauthorized modification

iv. Availability of information to authorized users when needed

v. Meet regulatory and legislative requirements

vi. Produce, maintain and test Business Continuity plans as far as practicable

vii. Train all staff on information security

viii. Report and investigate all breaches of information security and suspected weaknesses

ix. Monitor Risk Treatment Plan and measure effectiveness of selected controls.

When planning how to achieve its information security objectives, the organization shall monitor

- Uptime of servers and Networks
- Achievement of preventive maintenance planned schedule
- Closure of Nonconformities in defined time frame
- Conducting of defined no of awareness programme as per the process
- Monitoring of security incidents as per process of incident Management
- Mock drills of BCP as per process and achievement of targets:
- Review of risks as per defined process and closure of actions as per last review.

The templates for each one of them is defined and frequency and thresholds for each of them is defined in the template. For monitoring and analysis following

a) Monitoring and measurement of the controls shall be done as per process mentioned in the template.
b) System Administrator either himself or shall make one of the data center employee responsible for monitor and measurement of controls.

c) The results from monitoring and measurement shall be analyzed and evaluated at least on monthly basis. However, this analysis can be made early depending on the exigencies and system administrator shall decide the same.; and

d) System Administrator shall analyses and evaluate these results.

7 Support

7.1 Resources

The management provides resources for the implementation, maintenance, and review of the ISMS. The resources include funds, tools, human resources and any other resources that may be required for the efficient performance of the ISMS.

Periodically the NST (P) LTD. evaluates resource requirements for improvements in security infrastructure based on RA, review /audit records. Based on resource requirements, the Management approves/ allocates the required resources.

7.2 Competence

Personnel who have experience and expertise in the application domain and in information security concepts are assigned to manage ISMS. Whenever feasible, experienced individuals are available and allocated appropriate responsibilities. When the required levels of skill and expertise are not available, trainings are provided to ensure skill / knowledge enhancement as per the NST (P) LTD. training process. The ISMS training should form an integral part of training curriculum of HR Dept. in association with Co-ordination Team. Refer **'**PR-10-TRA-Training Process'

- Identifying what training is needed, and how frequently, for specific positions.
- Identifying qualified individuals/agency to conduct the training program.
- Organizing the training program.
- Maintaining attendance records, course outlines and course feedback of all trainings conducted.

The NST (P) LTD. maintains records of all training programs as mentioned in the training process.

7.3 Awareness

Persons doing work under the organization's control shall be aware of:

- the information security policy;
- their contribution to the effectiveness of the information security management system, including the benefits of improved information security performance; and
- The implications of not conforming to the information security management system requirements.
- All updates in organization policies & procedure, which are relevant to their job function

7.4 Communication

Users shall be made aware about the risk of Information Security while exchanging information through Voice, Email, Fax, and Video Communication facility.

What to communicate	When to communicate	With whom to communicate	Who shall communicate	Processes by which communication shall be effected
Technical matters	To seek clarification, communicate execution and discussing options of delivery	Customer	Delivery Manager / Technical Lead	Email / Video Call/Phone
Non-Technical Business Development	when communicating upgrades / updates and offers of NST	Customer	Account Manager	Email / Video Call/Phone
Financial Information such as Invoices, Payment reminder, Proposal, upgrade offer etc.	As and when the event takes place	Customer	Accounts Manager	Email / Video Call/Phone
Technical matters	To get the action initiated on completion of delivery	Accounts Manager / Business Head	Delivery Manager / Technical Lead	Email / Video Call/Phone
Performance report	Monthly / quarterly	Business Head	Account Manager and Delivery Manager	PPT / Word / Excel - Email/Phone
Technical Matters	As and when the event takes place	Project Manager	Developer/Tester	PPT / Word / Excel - Email/Phone

7.5 Documented information

7.5.1 General

The organization’s information security management system shall include:

a) Documented information required by this International Standard; and
b) Documented information determined by the organization as being necessary for the effectiveness of the information security management system.

NOTE: The extent of documented information for an information security management system can differ from one organization to another due to:

1. The size of organization and its type of activities, processes, products and services;
2. The complexity of processes and their interactions; and
3. The competence of persons.

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) Identification and description (e.g. a title, date, author, or reference number);
b) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) Review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and
b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

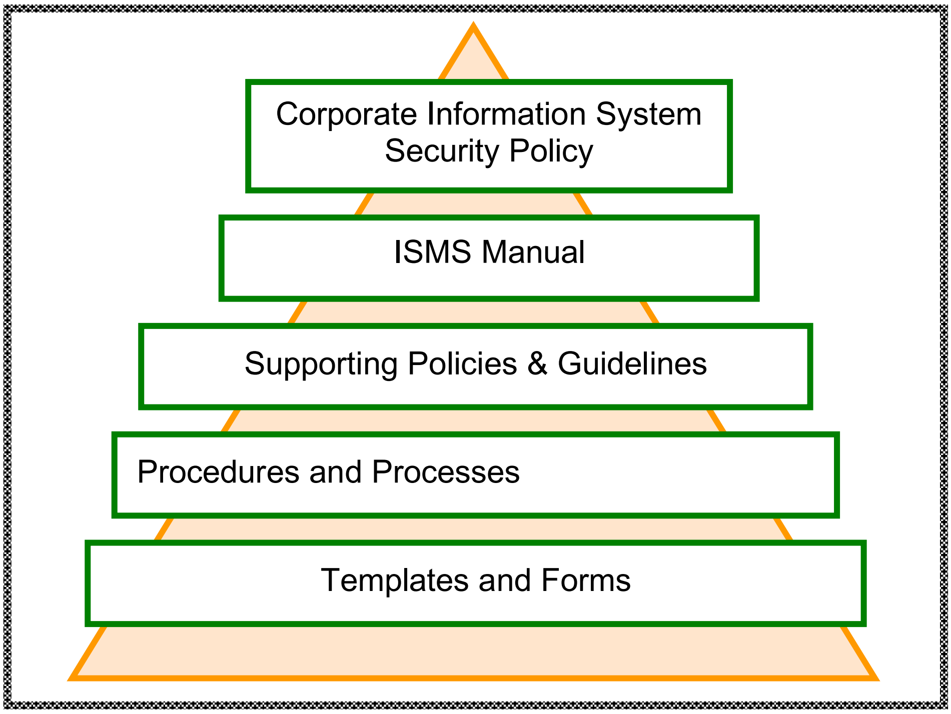
For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;
d) storage and preservation, including the preservation of legibility;
e) control of changes (e.g. version control); and
f) Retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

To meet the requirement of 7.5, the documentation structure of Information security management System is as detailed below:


Corporate Information System Security Policy
ISMS Manual
Supporting Policies & Guidelines
Procedures and Processes
Templates and Forms

The components of ISMS Documentation are:

Level - 0 Corporate Information System Security Policy): It is the Top-level security policy of the NST (P) LTD.

Level - 1 ISMS Manual): This document includes requirements of the ISO/IEC 27001:20132013 standard and describes how the defined ISMS meet the requirements. The document details the NST (P) LTD. approach towards management and implementation of ISMS.

Level - 2 Supporting Policies & Guidelines A complete set of supporting technical policies and guidelines as identified and defined by the NST (P) LTD. within the scope of ISMS.

Level - 3 Procedures and Processes – Contains processes and procedures required for implementing and supporting the defined policies & guidelines.

Level - 4 Templates and Forms –NST (P) LTD standard templates/forms used in the processes / procedures. These are used to streamline the operation of ISMS and form a basis for records.

Control of Documents

All documents related to ISMS requirements are controlled as per ‘NST-CP-03-ISMS-DRM-Document & Record Management Procedure’

This includes:

- Review and approval of documents for adequacy prior to issue / use
- Updating, review and approval of necessary changes in controlled documents
- Availability of current revisions of necessary documents
- Withdrawal of obsolete documents from all points of issue or use to ensure guarding against unintended use.
- All security documents are available on the Intranet for reference and use based on need-to-know requirements.
- Any document if printed is considered obsolete. However, this excludes all the documents related to ‘**Business Continuity Plan**

Control of Records

Records are identified within each procedure in the ISMS to provide evidence of conformance to requirements and effective functioning of the ISSC. Master list of records is maintained. Refer ‘PAL-Process Asset Library-Content Master’.

Other attributes shall be as per **‘**NST-PO-12-ISMS-CLH-Information Classification, Labeling and Handling Policy.docx’

8 Operation

8.1 Operational planning and control

8.1.1 Implement and Operate the ISMS
Selected control objectives, and controls that are a part of RTP are implemented effectively in NST (P) LTD and they are also capable of enabling prompt detection of and response to security incidents.

NST (P) LTD. ensures that proper training and awareness on ISMS are conducted, and appropriate resources are assigned to manage ISMS.

NST (P) LTD. maintains a suitable matrix of risk / incidence reduction against its major controls identified every year for monitoring purposes to ensure effectiveness of selected controls. Logs of risk reduction and/or incidence reduction are maintained for results comparison and reproduction.

8.1.2 Monitor and Review the ISMS

NST (P) LTD. ensures that ISMS is properly monitored and reviewed periodically.

a) For monitoring incidents, the NST (P) LTD. has a well-defined Incident Management Procedure, which ensures that all problems, errors identified during processing of any information are handled promptly and effectively, and breach of security is appropriately addressed. Refer **'**PR-19-ISMS-IMP-Incident Management Process**'**.

b) A process for conducting Management Reviews and audit procedure of ISMS exists. The focus of the review is to ensure that ISMS is effective, and all policies, controls and security objectives are in line with business requirements. The audit focuses on the compliance of NST (P) LTD.'s practices as defined in ISMS. Refer 'GD-14-SEPG & ISMS Plan'

c) Information System Security Committee reviews the level of residual and acceptable risks based on the changes in the deployed technology, new threats and vulnerabilities and business objectives. Refer 'NST-CP-05-ISMS-RART-Risk Assessment & Risk Treatment Procedure'

d) The controls at appropriate intervals are monitored against the logs generated to arrive at the current risk exposure. This is compared with previous risk level to verify the effectiveness of controls. Refer 'PR-16-ISMS-CEM-Control Effectiveness Measurement Process'

8.1.3 Maintain and Improve the ISMS

Based on the review reports and audit findings, appropriate corrective and preventive actions, as approved by the Information System Security Committee are implemented and incorporated into the ISMS. Inputs for improvement can be from:

- Audit Reports
- Management Review Reports
- Incident Reports
- RA report
- Business Changes (Objectives, process, industry practices, legal/regulatory, etc)
- Environmental Change (New threats and vulnerabilities, technology Changes, etc.)

NST (P) LTD. maintains all inputs in an improvement database available for internal use's (P) LTD. consolidates the inputs and reviews the ISMS for applicable improvements. For changes to be made, NST (P) LTD. prepares an action plan and communicates the results to all interested /affected parties. All improvements should be directed towards predefined organizational Business objectives.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a). The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan. The organization shall retain documented information of the results of the information security risk treatment.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

NST shall evaluate the information security performance and the effectiveness of the information security management system.

NST shall determine:

a) what needs to be monitored and measured, including information security processes and controls;
b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
c) The details of what needs to be measured is given in

NOTE: The methods selected should produce comparable and reproducible results to be considered valid.

d) Monitoring and measurement of the controls shall be done on daily basis.
e) System Administrator either himself or shall make one of the data center employee responsible for monitor and measurement of controls.
f) The results from monitoring and measurement shall be analyzed and evaluated at least on monthly basis. However, this analysis can be made early depending on the exigencies and system administrator shall decide the same.; and
g) System Administrator shall analyze and evaluate these results.

NST shall retain appropriate documented information as evidence of the monitoring and measurement results. The templates where these evidences are maintained are defined in "PR-16-ISMS-CEM-Control Effectiveness Measurement Process.docx"

9.2 Internal Audits

MR conducts internal ISMS audits quarterly to verify the adherence to ISMS. The audits are conducted to ensure that ISMS:

- Conforms to the requirements of the ISO/IEC 27001:2013 standard
- Ensure compliance with relevant legal, statutory and contractual requirements
- Conform to the identified information security requirements
- ISMS is effectively implemented and maintained
- Performs as expected

Security Audits are conducted in accordance with the audit procedure defined in 'NST-CP-06-ISMS-IAP-Internal Audit Procedure'**.** Trained personnel, not having direct responsibility of the activity being audited, shall conduct audits. MR with the help of HODs will ensure that any non-conformance found is closed. MR is responsible for planning, scheduling, organizing and maintaining records of these audits.

9.3 Management Review

Top management shall review information security management system once every three months, or on an event-driven basis, to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:

a) The status of actions from previous management reviews;
b) Changes in external and internal issues that are relevant to the information security management system;
c) Feedback on the information security performance, including trends in:
   1. nonconformities and corrective actions;
   2. monitoring and measurement results;
   3. audit results; and
   4. Fulfilment of information security objectives;
d) feedback from interested parties;
e) Results of risk assessment and status of risk treatment plan; and
f) Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

NST shall retain documented information as evidence of the results of management reviews.

10 Improvement

10.1 Non conformity and Corrective Action

When a nonconformity occurs, NST shall:

a) react to the nonconformity, and as applicable:
   1. take action to control and correct it; and
   2. deal with the consequences;
b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1. reviewing the nonconformity;
   2. determining the causes of the nonconformity; and
   3. determining if similar nonconformities exist, or could potentially occur;
c) implement any action needed;
d) Review the effectiveness of any corrective action taken; and
e) Make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. The organization shall retain documented information as evidence of:

f) The nature of the nonconformities and any subsequent actions taken, and
g) The results of any corrective action.

The procedure is created, for implementing and tracking the correcting action. Refer ‘NST-CP-01-CAPA-Corrective & Preventive Action Procedure’.

10.2 Continual Improvement

The NST (P) LTD. is responsible for continual improvement of the ISMS for suitability and effectiveness.

Inputs to continual improvement can be:

- Change in security policies and objectives
- Audit results and Management Review Reports
- Incident Reports
- Analysis of monitored events
- Corrective and Preventive Actions
- Business Changes
- Environmental Change (New threats and vulnerabilities)
- Best practices of industry

11 ISMS Controls

This section describes the selection and implementation of controls by NST (P) LTD.

The control objectives and controls listed in this section are directly derived from the ISO/IEC 27001:2013 standard, based on **'Section 5.3.1 - Security Domains addressed in ISMS'** of this document.

Controls applicable to NST (P) LTD. have been mentioned and addressed in this section.

Controls not applicable to NST (P) LTD. are mentioned in this section and exclusion with justification given in SOA. Refer 'NST-ISO27001-2013-SOA-V1.0.xlsx'

A.5 Information Security policies

A.5.1 Management Direction for Information Security

Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

A.5.1.1 Information Security Policy Document

A **Corporate Information System Security Policy** document approved by the management exists. Information security policy document called the **'ISMS Manual** has been published and communicated to all employees of NST (P) LTD., through the Intranet and mails, training and induction programs.

A.5.1.2 Review of the policies for information security

NST (P) LTD. is responsible for the creation, maintenance and updating of the policy. Information System Security Committee approves the policy prior to release. The review and evaluation of ISMS policy is conducted at least once in a year. The review guidelines state that the policy is to be reviewed against its effectiveness, compliance to business process, and compliance to technology changes. This is detailed in **section 9.3**.

A.6 Organization of Information Security

A.6.1 Internal organization

Control Objective: To manage information security within NST (P) LTD.

A.6.1.1 – Information Security Roles and responsibilities

Security roles and responsibilities of employees, contractors and third-party users are defined and documented in accordance with the organization's information security policy.

A.6.1.2 – Segregation of duties

In NST (P) LTD., duties have been segregated in order to reduce the risk of accidental or deliberate system misuse. Different individuals are responsible for their respective areas, and proper controls exist that take care of possibility of fraud in areas of single responsibility without being detected. Different areas and associated responsibilities are defined as per Roles and Responsibilities **Section 6.1.1**. Day to day administration & maintenance of IT Infrastructure is done by IT Department & HOF/IT review different logs & conduct periodic VA.

A.6.1.3– Contact with authorities

Appropriate contacts/ agreements are maintained with the following but not limited to:

Services	**Responsibility**
▪ Internet Service Provider (ISP)	Head/IT
▪ Hardware Maintenance contracts	Head/IT
▪ Telecom services department	Head/IT
▪ Electricity services department	Admin/HR
▪ Local Enforcement Agencies like Police, Fire	Admin/HR

Responsibility for any other services which fall under Information Security preview, but not mentioned above, is assigned to Head/IT. This is necessary to ensure that appropriate actions can be promptly taken, and advice obtained in the event of any security incident. Organization's legal department is consulted for all third party contracts and agreements.

A.6.1.4 – Contact with special interest groups

Information security advice is obtained from vendors, legal advisors and technical experts on security matters to maximize the effectiveness of the ISMS. Internally MR shall act as Security Advisor. External advice shall only be sought by MR if required. All security incidents and breaches are reported to MR for necessary corrective and preventive actions.

A.6.1.5 – Information Security in Project Management

Project Planning, Monitoring and Control shall take care of information security in project management, which is defined in PR-11-PMC-Project Planning and Project Monitoring and Control Process.doc

A.6.2 Mobile Devices and Tele Working

Control Objective: To ensure information security when using mobile computing and teleworking facilities.

A.6.2.1 – Mobile Device Policy

NST (P) LTD. has well defined policy and guidelines on the use of laptops. Refer 'PR-17-ISMS-AHP-Asset Handling Process.docx'. and NST-PO-19-ISMS-MDP-Mobile Device Policy.docx

A.6.2.2 – Teleworking

NST (P) LTD. has a well-defined policy and guideline on the use of laptops for teleworking purposes. Refer 'NST-PO-08-ISMS-VPN-Virtual Private Network Policy.docx'

A.7 Human Resource Security

A.7.1 Prior to employment

Control objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

A.7.1.1 –Screening

NST (P) LTD. has a documented recruitment process which includes background verification of employees above of certain grade or those working at critical position, immediately after joining.

The screening requirements form part of contract agreement with vendors.

A.7.1.2 – Terms and conditions of employment

All employees of, NST (P) LTD., at the time of joining, are required to agree and sign the Terms and Conditions of employment as detailed in **Recruitment Process.** The Terms and Conditions also state the employees' responsibility for Information Security.

A.7.2 During employment

Control Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

A.7.2.1 – Management responsibilities

Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

A.7.2.2 – Information security awareness, education and training

NST (P) LTD. Ensures that users (employees and the relevant external parties) are made aware of their security responsibilities through ongoing awareness training programs. All employees are to adhere them while executing the Roles and Responsibilities as defined.

A documented procedure for training exists. NST (P) LTD., in association with HR Dept. ensures that all, NST (P) LTD. personnel are imparted ISMS related training and that a training module on Information security policies becomes an integral part of induction training programs. Refer 'PR-10-TRA-Training Process'

A.7.2.3 – Disciplinary process

Any violation of the signed documents is considered as a disciplinary offence and as such act as a deterrent to employees who might otherwise be inclined to disregard security procedures. The procedure shall ensure correct, fair treatment for employees who are suspected of committing serious or persistent breaches of security. It is addressed by the reference to **NST (P) LTD. Conduct, Disciplinary and Appeal (CDA) Rules**. Refer "**Disciplinary Action Process**".

A.7.3 Termination or change of employment

Control Objective: To ensure that employees, contractors and third parties exit, NST (P) LTD. or change employment in an orderly manner.

A.7.3.1 – Termination or change of employment responsibilities

Responsibilities for performing employment termination or change of employment are clearly defined and assigned. Detailed exit form is filled to ensure return of assets, revocation of access rights, full & final settlement and Job handover by exiting employee and approved by relevant department heads, line /reporting manager and HR. No code sharing agreement is also signed by exiting employees related to solution department to ensure that confidentiality of information is maintained. Refer to **NST (P) LTD. Conduct, Disciplinary and Appeal (CDA) rules**.

A.8 Asset Management

A.8.1 Responsibility for assets

Control Objective: To achieve and maintain appropriate protection of NST (P) LTD and its assets.

A.8.1.1 – Inventory of assets

NST (P) LTD.'s Assets have been classified as:

- **Hardware** – Includes computer equipment (CPU, Peripherals etc.), communication equipment (routers, switches, etc.), magnetic media (CDs, Tapes, Disks), UPS/Inverters / power backup devices/Battery Bank, Air conditioner, Fire extinguisher etc.
  - **Software** – Includes various applications programs, system software, development tools and utilities.
  - **Information** –Databases, data files, archived information, documentation.
- **Services** – Include communication services, general utilities like power, AC, Buildings (Rent Agreement- Renewal) Services (provided by org external/internal the group) etc.
- **Management System- Includes Borrowed Information, Copyright/IPR, The whole Organization**
- **Human Resource- That include Technical** Manpower & Administrative manpower

An inventory of all assets is maintained by the IT department in the form of **Asset Register** NST (P) LTD. maintains appropriate protection of the organizational assets. It aims at confidentiality, integrity and availability.

A.8.1.2 – Ownership of assets

All information and assets associated with information processing facilities shall be owned by a designated part of the organization. The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has property rights to the asset.

A.8.1.3 – Acceptable use of assets

Rules for the acceptable use of information and assets associated with information processing facilities are identified, documented, and implemented. Ref to 'GD-21-ISMS-AUA-Acceptable Use of Assets Guidelines'

A.8.1.4 – Return of assets

All employees, contractors and third party users are required to return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

A.8.2 Information Classification

Control Objective: To ensure that information receives an appropriate level of protection.

A.8.2.1 – Classification of information

There are four levels of information classification defined in NST (P) LTD. Refer 'NST-PO-12-ISMS-CLH-Information Classification, Labeling and Handling Policy.docx'

A.8.2.2 –Labeling of information

The guidelines for labeling and handling of Information in NST (P) LTD. are documented and available in 'NST-PO-12-ISMS-CLH-Information Classification, Labeling and Handling Policy.docx'

A.8.2.3 –Handling of assets

NST (P) LTD. has well defined guidelines for information labeling, handling and storage in order to protect information from unauthorized disclosure or misuse. Refer 'NST-PO-12-ISMS-CLH-Information Classification, Labeling and Handling Policy.docx'

A.8.2.4 – Return of assets

All employees, contractors and third party users are required to return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

A.8.3 Media handling
Control Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruptions to business activities.

A.8.3.1 – Management of removable media

All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications. NST (P) LTD. has defined procedure for the management of computer media containing sensitive data. Refer 'PR-17-ISMS-AHP-Media Handling Process.docx'.

A.8.3.2 – Disposal of media

NST (P) LTD. has defined procedure for the disposal of computer media and other e-waste. The Tapes, CDs and Hard Disks have been covered in 'PR-17-ISMS-AHP-Media Handling Process.docx'.

A.8.3.3 – Physical media transfer

Backup media, Floppy, CD, Hardcopy etc. being transported from one location to the other is protected from unauthorized access, misuse and corruption by sending them through trusted, NST (P) LTD. employee with proper authorizatiofaccessn and adequate protection. Refer 'NST-PO-12-ISMS-CLH-Information Classification, Labeling and Handling Policy.docx'

A.9 Logical Security /Access Control

A.9.1 Business requirement for access control
Control Objective: To restrict access to information and information processing facilities.

A.9.1.1 – Access control policy

NST (P) LTD. has implemented access control to information based on the business requirements and security requirements on 'need-to-know' basis. Well-documented access control policy and procedures are in place including access to cloud services. Refer 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'

A.9.1.2 – Access to network and network services

The access to internal and external network of NST (P) LTD. is controlled. This includes any direct access to services that are business critical to users within the domain, and direct access to network from users in high-risk location like users through Internet. Users shall only have direct access to the services that they have been specifically authorized to use. Binding of IP address through MAC is enabled to ensure authorized access to network. A defined and documented policy for use of network services exists. Refer 'NST-PO-10-ISMS-IEM-Internet & Electronic Messaging Usage Policy.docx'.

A.9.2 User access management

Control Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

A.9.2.1 – User registration & deregistration

NST (P) LTD. has well defined policy and procedure for managing user access to all information systems and services. Refer 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'

A.9.2.2 – User access provisioning

A unique login id and password has been assigned to all users, with varying privileges, depending on roles, and requirements. User identification and authentication is implemented in accordance with privileges granted to the respective user. Refer 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'

A.9.2.3 – Management of Privileged Access rights (Password Policy)

The allocation and use of privileges is restricted and controlled. Any privilege given onto any system in NST (P) LTD. is covered. Refer 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'

A.9.2.4 – Management of Secrete Authentication information of users (Password Management)

NST (P) LTD. has a well-defined password policy and guidelines. Refer 'NST-PO-06-PP-Password Policy.docx'. 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'

A.9.2.5 – Review of user access rights

User privileges for NST will be reviewed every three months and for global users it will be reviewed once every year. System Administrator shall review the access rights & respective Business Owner shall ratify the review report.

A.9.2.6 – Removal or adjustment of access rights

The access rights of all employees, contractors and third party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

A.9.3 User Responsibilities
Control Objective: To prevent unauthorized user access, and compromise on theft of information and information processing facilities.

A.9.3.1 – Use of Secret Authentication Information

NST (P) LTD. has a well-defined password usage guideline for users to follow. It includes authentication to access cloud services also. Multifactor authentication and single sign on using O365 is implemented. Complex password is defined for VPN access. Refer 'NST-PO-06-PP-Password Policy.docx'. NST-PO-08-ISMS-VPN-Virtual Private Network Policy.docx

A.9.4 Operating system access control
Control Objective: To prevent unauthorized access to systems and applications.

A.9.4.1– Information access restriction

Unauthorized access to information is restricted. Refer 'PR-21-ISMS-ITO-IT Operation Process.docx', & 'PO-10-ISMS-IEM-Internet & Electronic Messaging Usage Policy'.

A.9.4.2 – Secure log-on procedures

All user machines are accessible through a user name and password. These are assigned to each authorized user and are unique in nature. Unauthorized access is not permitted. Refer 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx' NST-PO-16-ISMS-CON-Confidentiality Policy

A.9.4.3 – Password management system

NST (P) LTD. has a well-defined password policy and access management process. Refer 'NST-PO-06-PP-Password Policy.docx'. 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'.

A.9.4.4 – Use of system utilities (Privileged utility programs)

All system utility programs, which impact the operations of the systems, are installed with controlled access to administrative accounts. System Utilities are controlled.

A.9.4.5 – Access control to program source code

Source code and program libraries are not accessed by unauthorized people. Code management of IT related applications is being performed according to 'PR-08-SCM-Configuration Management Process'

A.10 Cryptography

A.10.1 Cryptographic Controls
Control Objective: To protect the confidentiality, authenticity, or integrity of information by cryptographic means.

A.10.1.1 – Policy on the use of cryptographic controls

NST-PO-15-ISMS-CCP-Cryptography Control Policy.docx

A.10.1.2 – Key Management

NST-PO-15-ISMS-CCP-Cryptography Control Policy.docx

A.11 Physical and environmental security

A.11.1 Secure areas

Control objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

A.11.1.1 – Physical security perimeter

NST (P) LTD. has a well-defined policy on physical security and procedure on physical access control. NST (P) LTD. has implemented different security barriers to check the access into the premises.

- NST (P) LTD. has main entry and exit point manned by security personnel.
- Entry to company premises for the employees is through biometric /access card and for visitors is through visitors pass.
- Access to specific /secure areas like server rooms is monitored through access card.
- Video Surveillance will be done through cameras installed at critical location.

A.11.1.2 – Physical entry controls

Secured areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

A.11.1.3 – Securing offices, rooms, and facilities

NST (P) LTD. has taken the following security measures:

- All employees, visitors and contract staff is supposed to report for security check-in and check-out formalities.
- Entry is restricted to authorize personnel through Biometric System.
- Each workstation, cubicle and cabin is provided with storage space, with lock and key arrangement to keep official documents/company classified information belonging to the employee of the workspace.
- Employees working after office hours enter their names, and sign –in and sign-out in a separate register maintained by the security guard on duty.
- Entire office facility is under CCTV surveillance which is monitored 24*7

A.11.1.4 – Protecting against external and environmental threats

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster are designed and applied.

A.11.1.5 – Working in secure areas

Physical protection and guidelines for working in secure areas are:

- Unsupervised work within server room will be strictly prohibited for safety reasons.
- Personnel shall only be aware of the existence of, or activities within, a secure area on a need to know basis
- Eating and consuming other food products will be strictly prohibited in secure areas.
- Photographic, video, audio or other recording equipment should not be allowed, unless authorized

A.11.1.6 – Delivery and loading areas

The delivery and handling of material is strictly under the authorization control with material gate pass. Without proper gate pass, no material is allowed to enter or leave the premises.

A.11.2 Equipment

Control Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

A.11.2.1 – Equipment sitting and protection

All equipment's are physically protected from security threats and environmental hazards, by positioning them at secure areas. Only authorized personnel can enter secured areas. The controls are adopted to minimize the risk of potential security threats. The following practices are being followed in NST (P) LTD.,

- Business critical equipment are installed in server room, which is fully secured under lock and key
- Fire and smoke alarms are deployed appropriately.
- The information processing and storage facilities are fully secured
- Users are not allowed to have drink, eatables & smoke in the server room.
- Temperature and humidity levels are continuously monitored and maintained.
- Power equipment is periodically serviced and checked.

The procedure for maintaining proper temperature and humidity is provided as per 'PR-21-ISMS-ITO-IT Operation Process'.

A.11.2.2 – Supporting utilities

All IT equipment's are protected from power failure and other electrical anomalies. Arrangements are made to provide uninterrupted power supply (UPS) to all critical information processing facilities. UPS are maintained as per the OEM's instructions and covered under AMC contract. Lighting protection is provided to the building. Adequate capacity of DG sets is available which are turned on in case of failure or routine power cuts.

A.11.2.3 – Cabling security

The power and data cables are well protected and isolated in order to protect from interception and damage. All the cables (data, telecommunication, and electrical) are laid using proper conduits, in order to protect them from external damage. Power cables and network cables are well separated to prevent any interference. Refer 'PR-21-ISMS-ITO-IT Operation Process'.

A.11.2.4 – Equipment maintenance

All equipment's in NST Server Room are being correctly maintained to ensure their continued availability and integrity. Adhering to the following steps ensures this:

- All equipment's are maintained in accordance with the OEM's recommendations for service intervals and specifications.
- All critical equipment's are covered under AMC.
- All equipment's are under the regular preventive maintenance.

A.11.2.5 – Removal of assets

All the equipment's that are taken out of the NST follow a proper authorization process. A proper gate pass is to be signed by the IT Manager before taking any equipment out of the NST.

A.11.2.6 – Security of equipment and assets off- premises

The person carrying the equipment outside the premises is responsible for the security of the equipment. NST (P) LTD. has a documented policy for Laptops and portable media taken outside premises. Refer 'PR-17-ISMS-AHP-Asset Handling Process.docx'.

A.11.2.7 – Secure disposal or re-use of equipment

The information available on equipment's is removed or erased before the equipment disposal. The information available on equipment's, which is re-used for some other purposes, is removed or erased before the equipment is re-used. The information available on media, which is re-used for some other purposes, is removed or erased before the media is re-used. All defective computer media, to be disposed, is destroyed completely and all relevant information is made irrecoverable. Refer 'PR-17-ISMS-AHP-Asset Handling Process.docx'.

A.11.2.8 – Unattended user equipment

A well-defined policy exists at NST (P) LTD. regarding equipment's unattended for a long duration. Refer 'NST-PO-07-ISMS-ACP-IT Access control Policy.docx'

A.11.2.9 – Clear Desk and Clear screen policy

Personal computers are not left logged on when not in use and are protected by password. The screen saver is password protected. Refer 'NST-PO-04-ISMS-CDCS-Clear Desk & Clear Screen Policy.docx'.

A.12 Operations Security

A.12.1 Operational procedures and responsibilities

Control Objective: To ensure the correct and secure operation of information processing facilities.

A.12.1.1 – Documented operating procedures

NST (P) LTD. has a set of defined operating manuals for processing the department functionality. All documented operating manuals are identified in the 'PAL-Process Asset Library-Content Master'.

A.12.1.2 –Change management

Whenever a change in the IT infrastructure is to be done, a proper evaluation and analysis is done which includes cost, security, technical functionality and compatibility. Any user can initiate change request. Manager/IT is authorized to initiate the change & Head/IT approves these operational and process changes. To control all operational changes NST (P) LTD. has defined policy. Refer 'PR-08-SCM-Configuration Management Process'

A.12.1.3 – Capacity management

It is the responsibility of the individual managers to look for capacity demands for their projects in advance. This ensures that the required capacity can be arranged in time to minimize the risk of failure due to lack of capacity. It also ensures the continuous availability of operational systems. Utilization of existing resources is monitored regularly. Refer 'NST-CP-04-ISMS-HSA-Hardware and Software Augmentation Procedure.docx'.

A.12.1.4 – Separation of development, test and operational facilities

The development and testing activities shall not be done in production server.

A.12.2 Protection from Malware

Control Objective: To protect the integrity of software and information processing facilities are protected against malware.

A.12.2.1 – Controls against malicious code

Precautions are required to prevent and detect the introduction of malicious software. Software information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses, and logic bombs etc. NST (P) LTD. has implemented several controls to address the threat:

- NST (P) LTD. has a policy for prevention against malicious software.
- NST (P) LTD. has a policy for the use of networks or any other medium as a preventive measure against virus attacks.
- Virus attacks and software malfunctions due to malicious software are treated as security incidents and handled.
- To prevent loss of data due to malicious software regular backups of critical data are taken regularly.

  Bitdefender antivirus is used to ensure the above

  Refer 'NST-PO-11-ANT-Antivirus Policy.doc'

A.12.3 Back-up

Control Objective: To maintain the integrity and availability of information and information processing facilities.

A.12.3.1 – Information back up

Backup of informational Servers are taken regularly. NST (P) LTD. has a well-defined procedure for Information backup and restoration. Refer 'NST-PO-09-BCK-Backup Policy.docx'.

A.12.4 Logging and Monitoring

Control Objective: To detect unauthorized information processing activities

A.12.4.1 – Event logging

NST (P) LTD. has defined policy for event logs. All systems are monitored to detect deviation from access control policy. This audit trail serves as evidence in case of security breach, and is the basis for any action. Audit logs are maintained on servers and provide audit information related to User Id, Date and time of log-on and log-off, failed login attempts, Terminal Location. Refer 'NST-PO-13-ISMS-NSM-Network Security Management Policy.docx'.

A.12.4.2 – Protection of log information

Logging facilities and log information are protected against tampering and unauthorized access.

A.12.4.3 – Administrator and operator logs

Logging facilities and log information are protected against tampering and unauthorized access.

A.12.4.4 – Clock synchronization

The correct setting of critical computer clocks is important and carried out to ensure the accuracy of audit logs, which may be required for investigation or as evidence in legal or disciplinary cases. One Server is identified as Time Master Server & other Servers of the network are synchronized with the Master.

A.12.5 Control of operational software

Control Objective: To ensure the integrity of operational systems.

A.12.5.1 – Installation of software on operational systems

To ensure secured implementation of Software on Operational System. Refer ‘NST-CP-04-ISMS-HSA-Hardware and Software Augmentation Procedure.docx’

A.12.6 Technical Vulnerability Management

Control objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

A.12.6.1 – Management of technical vulnerabilities

NST (P) LTD. is using VA/PT to obtain information on new exposures while applying patches for earlier identified threats and vulnerabilities. The VA/PT shall be carried out as per Security Committee Review Procedure. Appropriate actions will be initiated based on threat assessment diagnosed from VA/PT.

A.12.6.2 – Restrictions on software installation

Users should not run any unauthorized or undocumented software on their desktops. IT department will approve on the recommendation of Department Heads, the installation of any software on Desktop/Laptop/Servers. “PR-17-ISMS-AHP-Asset Handling Process.docx” in section 7. Guidelines for Desktop/Laptop/Server users

A.12.7 Information systems audit considerations

Control Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

A.12.7.1- Information systems audit controls

Audit activities involving checks on operational system shall be carefully planned and agreed to minimize the risk of disruption to business processes.

A.13 Communications and Operations Management

A.13.1 Network security management

Control Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

A.13.1.1 – Network controls

NST (P) LTD. has a dedicated team of employed professionals in network, who are responsible for the smooth and secure operation of the network. Policies of network and cloud services usage are defined. Refer 'NST-PO-10-ISMS-IEM-Internet & Electronic Messaging Usage Policy.docx'.

A.13.1.2 – Security of network services

Security attributes for network services like Leased Line / Wireless Radio modem is taken care through SLA (Service Level Agreement) with ISP (Internet Service Provider) viz., STPI.

A.13.1.3 – Segregation in networks

Network is segregated as per policy defined in 'NST-PO-13-ISMS-NSM-Network Security Management Policy'**.** Subnet are configured for secure and effective communication.

A.13.2 Exchange of Information

Control Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

A.13.2.1 – Information transfer policies and procedures

The Electronic Office Systems like Telephone, Fax etc. are maintained by a 3rd Party. Security of Information available through such system is ensured through suitable clauses in the contract.

Users shall be made aware about the risk of Information Security while exchanging information through Voice, Fax, and Video Communication facility.

A.13.2.2 – Agreements on information transfer

Agreements shall be established for the exchange of information and software between NST and external parties like Oracle, MS, and IBM etc.

A.13.2.3– Electronic messaging

The electronic mail systems are properly secured from unauthorized access by using Spam protection software & Anti-Virus firewall, and from viruses by deploying antivirus software. NST (P) LTD. has a well-defined policy and guidelines on the use of electronic mail. Refer 'NST-PO-10-ISMS-IEM-Internet & Electronic Messaging Usage Policy.docx'.

A.13.2.4 – Confidentiality or non-disclosure agreements

All contractors and external parties are required to sign NDA as covered by respective contract guidelines. Certain projects may also require signing of separate NDA between employee and customer.

A.14 Systems acquisition, development and maintenance

A.14.1 Security requirements of information systems

Control Objective: To ensure that security is an integral part of information systems.

A.14.1.1 – Security requirements analysis and specification

NST (P) LTD., will acquire and accept hardware and software. Refer 'NST-CP-04-ISMS-HSA-Hardware and Software Augmentation Procedure.docx'

A.14.1.2 – Securing applications services on public networks

NOT APPLICABLE.
AS PER SOA

A.14.1.3 – Protecting application services transactions

NOT APPLICABLE.
AS PER SOA

A.14.2 Security in development and support processes
Control Objective: To maintain the security of application system software and information.

A.14.2.1 – Secure development policy

Software development will be as per the agreed Software Development Lifecycle defined in "PR-09-SLC-Software Life Cycle Process.doc"

A.14.2.2 – Change control procedures

NST (P) LTD. has a defined procedure to manage and control changes in the software developed and support systems, during the development life cycle. Refer 'PR-08-SCM-Configuration Management Process'

A. 14.2.3 – Technical review of applications after operating system changes

The application systems are reviewed to ensure that there is no adverse impact on operation and security due to changes in operating system. Refer 'PR-08-SCM-Configuration Management Process'

A. 14.2.4 – Restrictions on changes to software packages

Modification to software package is not permitted without the consent of project team. To ensure that only desired changes are implemented after the approval, a process need to be followed for controlling the changes in software packages. For this the process is defined 'PR-08-SCM-Configuration Management Process'

A. 14.2.5 – Secure System Engineering Principles

Software development will be as per the agreed Software Development Lifecycle defined in "PR-09-SLC-Software Life Cycle Process.doc"

A. 14.2.6 – Secure Development Environment

To secure the selected product of development environment the process of configuration management need to be adopted so that the correct product is available to authenticated users. For this the process is defined 'PR-08-SCM-Configuration Management Process'

A.14.2.7 – Outsourced software development

NOT APPLICABLE. AS PER SOA

A. 14.2.8 – System security testing

System security testing process is defined in section 7.3 of GD-04-TEST-Testing Guidelines.doc

A.14.2.9 – System acceptance testing

New information systems, upgrades, and new versions are put through a system acceptance for their acceptability and interoperability. A separate environment comprising of hardware and software is used to carry out tests prior to deploying or upgrading the main system. Appropriate tests are carried out to confirm that all acceptance criteria are fully satisfied. The tests results are documented and operational, maintenance and usage procedure are established. Training is provided for use and operation of new system. Refer ‘NST-CP-04-ISMS-HSA-Hardware and Software Augmentation Procedure.docx’

A.14.3 Test Data

Control Objective: To ensure the protection of data used for testing.

A.14.3.1 – Protection of test data

System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data, hence test data is carefully selected and controlled such that security violations do not occur. Refer ‘NST-CP-04-ISMS-HSA-Hardware and Software Augmentation Procedure.docx’

A.15 Supplier relationships

A.15.1 Security in supplier relationship

Control Objective: To maintain the security of NST (P) LTD.’s information and information processing facilities that are assessed, processed, communicated to, or managed by external parties or suppliers.

A.15.1.1 – Information security policy for supplier relationships

NST has identified risks from third-party access mainly in two categories viz., Physical and Network. Risk areas have been identified and appropriate measures shall be taken to mitigate them. They have been addressed adequately in the following sections of this chapter.

- **A.11.1.2 – Physical entry controls**
- **A.9.1.2 – Access to network and network services**

All contract personnel are given restricted access as per the requirement of the service they are providing and as per the contractual obligations. All third parties working at the premises have signed Non-Disclosure Agreement (NDA) at the time of contracts.

A.15.1.2 – Addressing security within supplier agreements

All agreements with the supplier who provides any type of services to NST & have access to the premises of NST shall have a clause related to security and Access Control as under
"The vendor will adhere to security guidelines of NST while delivering the services and follow access privileges & rights provided with precaution and safety measures indicated for each of them. Non-adherence of these guidelines may result in termination of the agreement and/ or claiming of liability/ damages caused due to non-adherence of these instruction."

A.15.1.3 – ICT (Information and Communication Technology) Supply chain

All agreements with the Information & Communication Technology service provider, who provides any such type of services to NST, shall have the requirements to address information security risk in the agreement.

A.15.2 Supplier service delivery management

Control Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 – Monitoring and review of supplier services

The services, reports and records provided by the third party are regularly monitored and reviewed regularly. SAP workflow is used to manage the end to end procurement process. Purchase directly through OEM is preferred for better quality of products and services. Online purchase is also facilitated for competitive pricing and faster delivery.

A.15.2.2 – Managing changes to supplier services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Control Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

A.16.1.1 – Responsibilities and procedures

Incident management responsibilities and procedure exist to ensure a quick, effective, and orderly response to security incidents. Refer **'PR-19-ISMS-IMP-Incident Management Process'**.

A.16.1.2 – Reporting information security events

Security events are defined as incidents that could cause unauthorized disclosure, modification, or destruction of, NST (P) LTD.'s information assets, or loss or destruction of the physical equipment associated with the computer systems, it's peripheral or network infrastructure components. Security incidents also include other aspects of security, such as carrying fire arms, or other lethal weapons on property, are as typically secured being left unlocked or unattended, fire or hazardous material spills, or witnessing someone performing an unsafe act, or committing a violation of security policies or procedures etc. All users in the, NST (P) LTD are responsible to report any observed or suspected security incidents through email/help desk phone/on-line Incident reporting system available on Intranet. The security incidents are reported and are managed by the documented procedure. Refer ‘PR-19-ISMS-IMP-Incident Management Process’.

A.16.1.3 – Reporting information security weaknesses

Security weaknesses are defined as loopholes, weak points or vulnerabilities in the information system. These vulnerabilities or the loopholes may be exploited to gain unauthorized access to data or systems. All users in the, NST (P) LTD. are responsible to note and report any such observed or suspected security weakness. Any user (viz., employee, contractor and third party) can report the incident using email/help desk phone/online system available on Intranet. They shall report these incidents as per ‘PR-19-ISMS-IMP-Incident Management Process’.

A.16.1.4 – Assessment and decision of information security events

All incidents occurring in the, NST (P) LTD. are documented and stored and handled as per the procedure defined in PR-19-ISMS-IMP-Incident Management Process.docx

A.16.1.5 – Response to information security incidents

All incidents occurring in the, NST (P) LTD. are documented and stored and handled as per the procedure defined in PR-19-ISMS-IMP-Incident Management Process.docx

A.16.1.6 – Learning from information security incidents

All incidents occurring in the, NST (P) LTD. are documented and stored in the Corrective and Preventive Actions database. The , NST (P) LTD. consolidates the incident reports for root cause analysis and considers these as an input for appropriate actions and necessary controls to avoid reoccurrence of the incidents.

A.16.1.7 – Collection of evidence

All applicable laws and regulations have been identified by, NST (P) LTD. wherever applicable, the records and documents that may be accepted as evidence shall be collected and maintained. Shall ensure that all evidence collected in the process is:

- Admissible as evidence – Acceptable to court and legal authorities
- Complete – Present a complete trail of the incident
- Meet quality requirements – Are readable, legible etc.

A.17 Business continuity management

A.17.1 Information security aspects of business continuity management

Control objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure timely resumption.

A.17.1.1 – Planning information security continuity

Business continuity begins by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This is followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). This assessment considers all business processes and is not limited to the information processing facilities. Depending on the results of the risk assessment, a strategy plan is developed to determine the overall approach to business continuity. The details of BCP are detailed as per **‘PR-22-ISMS-BCP-Business Continuity Plan Process’.**

A.17.1.2 – Implementing information security continuity

Implementing information security continuity shall covered in section 6.2.Identify critical resources & in section 7.2. Business Continuity Policies for the Organization in PR-22-ISMS-BCP-Business Continuity Plan Process.docx

A.17.1.3 – Verify, review and evaluate information security continuity

Business continuity plans shall be tested regularly to ensure that they are up to date and effective. Such tests should also ensure that all members of the recovery team and other relevant staff are aware of the plans. The test schedule for business continuity plan(s) are detailed in the **‘PR-22-ISMS-BCP-Business Continuity Plan Process’.**

A.17.2 Redundancies

Control objective: To ensure availability of information processing facilities.

A.17.2.1 – Availability of information processing facilities

Information processing facilities shall be monitored, and sufficient redundancy shall be ensured by fixing the appropriate threshold level while maintain Control Effectiveness Measurement as defined in the PR-16-ISMS-CEM-Control Effectiveness Measurement Process. Firewall policy are configured to ensure High Availability (HA)

A.18 Compliance

A.18.1 Information security reviews

Control Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

A.18.1.1 – Independent review of information security

Information System Security Committee is responsible for reviewing and auditing the ISMS for its compliance. All areas covered in the ISMS policy are considered for regular reviews and audits. MR prepares and publishes the annual audit/ review plan. Details are mentioned in **Section 6** of this document.

A.18.1.2 – Compliance with security policies and standards

The , NST (P) LTD. with the help of the Security Committee and other Core Group members conducts periodic/event-driven review to ensure compliance with security policy & standards.

A.18.1.3 – Technical compliance checking

Periodic internal audits, third party audits and independent VA/PT shall be planned for and conducted according to Security Committee Review Procedure.

A.18.2 Compliance with legal and contractual requirement

Control Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.

A.18.2.1 – Identification of applicable legislation

All relevant statutory, regulatory, and contractual obligations pertaining to information systems are explicitly defined and documented. NST (P) LTD. adheres to all the applicable laws and acts. It is the responsibility of the HR department to review compliance and identify new or unidentified legal obligations. All agreements entered by the company are duly vetted and approved by the HR department for this purpose.

A.18.2.2 – Intellectual property rights (IPR)

NST (P) LTD. ensures that all license agreements are respected and limits the use of the products to specified machines, and for specific purposes.

a) The IPR of hardware, software and documentation belonging to , NST (P) LTD. will not be disclosed to any outside party unless and otherwise cleared by , NST (P) LTD.

b) The IPR of programs and associated material supplied by outside organizations / collaborators will be used by, NST (P) LTD. for only those purposes for which they are licensed.

c) No unauthorized copies will be made for use within or outside, NST (P) LTD.

A.18.2.3 – Protection of documented information

The important records are protected from loss, destruction and falsification. The following records of, NST (P) LTD. are safeguarded:

- Master List of Documents
- Master List of Records
- Database records
- Transaction logs
- All contracts and agreements

All records are retained for a defined period as specified by the owner of the information. Storage and handling of all these records is in accordance with a defined procedure. Refer ‘PR-24-ISMS-COM-Complinace Process.docx’

A.18.2.4 – Privacy and protection of personal information

Data protection Act is not applicable in (P). However, all personal records are maintained as hard copies and classified as ‘Confidential’. Only HR department has access to those files. Online personal information is maintained which is password protected, and the access is limited to the HR.

A.18.2.5 – Regulation of cryptographic controls

The cryptographic regulations as per IT Act 2000 of Government of (P) shall be followed for NST operations. In case of usage of third party cryptographic devices compliance letter from the third party shall be secured.

12. ISMS Master list of Records and its Retention Period

Sl. No	Record Name	Responsibility	Classification of Information	Retention Period
1.	Security Council Meeting Minutes	MR	Restricted	1 Year
2.	Corrective Action Record	MR	Restricted	1Year
3.	Preventive Action Record	MR	Restricted	1 Year
4.	User Registration & Deregistration Record	IT Manager	Restricted	1 Year
5.	Incident Log	MR	Restricted	3 Years
6 .	Asset Record	MR	Restricted	3 Years
7.	Risk Assessment Record	MR	Restricted	3 Years
8.	List of Applicable Legislations	MR	Restricted	3 Years
9.	Server Logs	System Administrator	Internal	1 Year
10.	NC Reports	MR	Restricted	3 Years
11.	BCP Record	IT Manager	Restricted	3 Years
12.	Change Request Record	System Admin	Internal	3 Years
13.	Change Request Impact Analysis Record	System Admin	Internal	3 Years
14.	Software License Usage Monitoring Report	System Admin	Internal	1 Year
15.	Bandwidth Monitoring Report	System Admin	Internal	6 Months
16.	H/W and S/W Verification Records	System Admin	Internal	1 Year
17.	List of authorized persons for sensitive data	MR/CISO	Restricted	1 Year
18.	Antivirus record of user machines	System Admin	Internal	1 Year
19.	Backup logs	System Admin	Internal	1 Year
20.	Backup restoration logs	System Admin	Internal	1 Year
21.	Network Access Authorization Records	System Admin	Restricted	1 Year
22.	Media Disposal Records	MR	Internal	3 Years
23.	Visitor Logbook	Admin	Internal	3 Years
24.	Contract for Power Supply	Admin	Internal	
25.	Contract for DG Set	Admin	Internal	
26.	Contract for Air Conditioner	Admin	Internal	
27.	Contract for Security Agency	Admin	Internal	
28.	Contract for Fire prevention	Admin	Internal	
29.	Contract for Leased Line	Admin	Internal	3 Years
30.	Contract for FM	Admin	Internal	
31.	Contract for Antivirus Protection	IT Manager	Internal	1 Year
32.	Third Party Contract & NDA documents	MR/ IT Manager	Restricted	3 Years
33.	IBM/MacAfee Service Level Agreement	IT Manager	Restricted	3 Years
34.	Background Verification Record	HR	Confidential	
35.	KPI related records	HR	Internal	
36.	ISMS Plan	MR	Internal	