

**Network Security Management Policy**

**Version History:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Date** | **Description of Change** | **Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 3rd Sep2013 | First Draft | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.0 | 30th Sep 2013 | Initial Release | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |

**Table of Contents**

[1. Objectives 4](#_Toc373854297)

[2. Scope 4](#_Toc373854298)

[3. Network Controls 4](#_Toc373854299)

[4. Communication and Operations Security Policy 4](#_Toc373854300)

[4.1 Network Management 4](#_Toc373854305)

[4.2 System Planning and Acceptance 5](#_Toc373854306)

[4.3 Network Communication Security 5](#_Toc373854307)

[4.4 Connectivity 5](#_Toc373854308)

[4.5 Information Exchange and Security 5](#_Toc373854309)

[4.6 Network Segregation 5](#_Toc373854310)

[4.7 Network Access policy for external devices 6](#_Toc373854311)

# Objectives

Communication links make up the arterial system of NST network on which the data and information transfer takes place. If we look around the wired system and the networks today, we will find that most of the risks and threats arise out the networked machines only and propagate through the communications links. Hence it will be very much required to have adequate operational procedures and controls to secure communications links. To protect the network services from unauthorized access.

# Scope

Communication and Operations policy applies to all the employees, vendors, business partners, and all those who work with the information processing systems and facilities of NST.

# Network Controls

* IT department will ensure that adequate security procedures and controls are developed and deployed to ensure security of the information and software being exchanged through insecure communication lines
* IT department will be responsible for the administration of the network of the NST, from a central location
* IT department will designate a person as ‘Network Administrator’. This person will also be the designate “Owner’ of the NST network equipment.
* Network Administrator will maintain a list of personnel from the IT department; the third party vendors and others who can access the routers and other network devices including security devices.
* Network Administrator will be responsible for monitoring security and for smooth functioning of the network.
* Administrative privilege to all the routers of NST will be provided to the Network Administrator only.

# Communication and Operations Security Policy

1.
2.
3.
4.

## Network Management

* IT Head will ensure that the responsibilities for operating and managing the network and the networked facilities are clearly defined and documented.
* The network operations and management procedures will also be supported by adequate and appropriate incident response procedures.
* IT Head will define and deploy appropriate procedures and controls to ensure security of data in transit and to protect networked services and resources.

## System Planning and Acceptance

* IT Head will ensure that adequate system and network monitoring is carried out to avoid any risk arising out of failure of a system/network due to inadequate capacity.
* Capacity planning will also be conducted for all new systems being acquired and all new hardware/software will have to meet the defined acceptance criteria, as specified from time to time.

## Network Communication Security

* Network Administrator will use access control lists on routers.
* Any sort of greeting or any other information will not be displayed on any connection originating from external sources until the user will be authenticated through a sign-on sequence that requires a unique user ID and password.
* All the server access will be logged and the log files thus generated will never be

## Connectivity

* If the business requirement arises, connectivity from other networks and computer system with NST network must be approved by line Manager.
* All unused connections and network segments will be disconnected from active networks.
* Functional/department heads will authorize the connectivity of third party laptops to any unused ports only after approval from IT Head.
* Internet access will be allowed to critical application/database server/ file server or server hosting sensitive data only on business requirements with proper security measures incorporated.
* No desktop/s or laptop/s will be allowed to connect to the critical server LAN, in case of any such requirement the permission from the functional/departmental head of respective application servers in that LAN and the Network Administrator will be taken and informed to line manager.
* In case of failure of any WAN connectivity causing business loss, proper escalation will be done and the same will also be informed to the business heads.
* Periodical LAN/WAN utilization report will be generated to monitor to identify or analysis future requirement of link bandwidth.

## Information Exchange and Security

* Organization will designate an officer to exercise control over the movement and usage of the removable storage media used for the purpose of taking data backup.
* It will be the prime duty of the designate officer to ensure that only authorized staff will have access to the removable storage media.

## Network Access policy for external devices

To provide network access to external devices, Project Manager will raise a service request on Service Request tracker (EMP) portal or email. Network Administrator will validate the request and then provide access to the external device.

## Network Segregation

Network has been segregated based upon the

* Rights permitted as per the application requirement
* Rules defined in the firewall
* Policies defined to share other networks for ex- (Gmail & Social networks)