

NST IT Operations Process

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver.** | **Date** | **Description of Change** | **Authored / Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 29th Aug 2013 | First Draft | Saket | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.0 | 30th Sep 2013 | Approved and Baseline | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.1 | 16th May 2016 | Update section 4.2.1 for Server room temperature | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.2 | 29th July 2015 | Update section 16.a for limit on size of incoming and outgoing mail messages. Earlier it was 5 Mb but now it increased. | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.3 | 5th Feb 2018 | Update section 6.0 for User registration and section 6.2 for User-Id Scheme for creating Email users’ user-id on the Mail Server | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.4 | 12th Sep 2019 | Update section 7.0 for Azure Data backup | Saket Madan | Dhananjay Kumar | Ajay Kr. Zalpuri |
| 1.5 | 28th Sep 2020 | Update section 18 for Privilege Management for Access in special circumstances | Rahul Raj | Tanuj/Saket | SEPG Team |

**Table of Contents**

[1 Introduction 4](#_Toc40286791)

[2 Scope 4](#_Toc40286792)

[3 Access to Server Room 4](#_Toc40286793)

[4 System 4](#_Toc40286794)

[4.1 System Availability 4](#_Toc40286795)

[4.2 Server Room Environment 4](#_Toc40286796)

[4.2.1 Temperature 4](#_Toc40286797)

[4.2.2 Humidity 5](#_Toc40286798)

[4.3 Power 5](#_Toc40286799)

[4.3.1 Server Room 5](#_Toc40286800)

[4.3.2 Power to Network Equipment 5](#_Toc40286801)

[5 Shutting Down of System 5](#_Toc40286802)

[5.1 Linux & UNIX Servers 5](#_Toc40286803)

[5.2 Windows Family Server 5](#_Toc40286804)

[6 User Registration 6](#_Toc40286805)

[6.1 User Registration 6](#_Toc40286806)

[6.2 User-Id Scheme 6](#_Toc40286807)

[6.3 User Deregistration 6](#_Toc40286808)

[7 Backup Operation 7](#_Toc40286809)

[8 Backup Media Labeling 7](#_Toc40286810)

[9 Backup Recovery & Testing 7](#_Toc40286811)

[10 Backup Media Management 7](#_Toc40286812)

[11 First-Aid & Fire-Fighting Practices 7](#_Toc40286813)

[12 Internet Infrastructure 8](#_Toc40286814)

[12.1 Procedure to Check Internet Services 8](#_Toc40286815)

[13 Network Infrastructure 8](#_Toc40286816)

[14 Monitoring System & Use 9](#_Toc40286817)

[15 Software Media Management 9](#_Toc40286818)

[16 E-Mail System 10](#_Toc40286819)

[17 Publicly Available Information 10](#_Toc40286820)

[18 Privilege Management 10](#_Toc40286821)

[19 Clock Synchronization 11](#_Toc40286822)

# Introduction

The objective of this procedure is to provide the setup and operational details of server rooms to ensure its secure and safe operations.

# Scope

This scope is limited to the activities being carried out in the operation of

* Linux based Server
* Windows based Servers
* Router and switch
* Storage Devices
* Internet Infrastructure
* Network Infrastructure
* Digital video recorder
* EPBAX

# Access to Server Room

Only Authorized persons shall have access to Server Room. Server room has access control for controlling the entry of any unauthorized person. Visitor’s entry is done in the logbook maintained inside the server room. This scope is limited to the activities being carried out in the operation of

* Linux based Server
* Windows based Servers
* Router and switch
* Storage Devices
* Internet Infrastructure
* Digital video recorder
* EPBAX

# System

## System Availability

System shall be available for 24x7 hours.

## Server Room Environment

### Temperature

1. Server Room Temperature range shall be maintained at 22 +2-degree C. The permissible temperature range for the system is 17 to 27-degree C.
2. The authorized person shall record the temperature reading once in a day and the Environment monitoring log will be maintained. If the temperature varies beyond the maintained temperature the air conditioning personnel shall take corrective measure. If the temperature varies beyond the permissible range, system shall be closed. Any incident that is reported is recorder and tracked in Incident Tracker Log.

### Humidity

1. Computer Room Humidity range shall be maintained at 50 +5% (non-condensing). The permissible humidity range for the system is 45% to 65% (non-condensing).
2. The authorized person shall record the humidity reading once in a day and the Environment monitoring log will be maintained. If the humidity varies beyond the maintained humidity range the air conditioning personnel shall take corrective measure. If the humidity varies beyond the permissible range, system shall be closed. Any incident that is reported is recorder and tracked in Incident Tracker Log.

## Power

### Server Room

1. AC voltage shall be maintained between 200-240 Volts. Necessary
   * 1. Controls are provided in the Electrical control panel.
2. Power to systems shall be given through UPS.
3. Load level of the UPS should maintain at 60%.
4. UPS shall be monitored for any faulty signals/alarms. If any fault arises, it shall be logged in and Service provider shall be informed.
5. Critical equipment’s in server room, will be on redundant power supply (RPS) and it will be powered by dual UPS in failover/load sharing mode.
6. UPS and batteries are to be kept separately from server room.

### Power to Network Equipment

Power to all Network equipment’s shall be through UPS.

# Shutting Down of System

## 5.1 Linux & UNIX Servers

Authorized person shall follow the procedure for shutdown:

1. Give shutdown command.
2. When system is down or halt message appears on console, switch off the power and monitor.
3. In case of problem, entry in logbook and inform IT In charge.

## 5.2 Windows Family Server

1. Logon to server.
2. Select Shutdown option on the Screen.
3. System will start shutdown and after shutdown system will automatically switch off its power.
4. If any machine is locked, and cannot be unlocked without administrative access, inform IT in-charge for necessary instructions.

# User Registration

# User Registration

1. HR/PMO shall raise a request to IT team to register user.
2. User shall be allotted a user-id and password by the IT team.
3. The user-id shall be allotted to individual user. However, group user-id may be allotted for some common application for publicly available systems.
4. The details of user – Full Name, Department, Manager name, and Phone No. shall be included in the user-id description. Common Application user-id shall have application name as user-id’s description for e.g., Sonicwallsupport user-id ‘sonicwallsupport@svam.com have description as A record of the users' registration shall be maintained.

## 6.2 User-Id Scheme

1. Email users’ user-id on the Mail Server comprises on following scenario
   1. First name initial and last name based on users’ name/initials. If incase the first name and last name combination exists, the extra character will be added.
   2. First Name Last Name
   3. Last Name First Name Initial
   4. First Name initial (.) Last Name
2. Single sign on policy for email, internet and business application is in place.

## 6.3 User Deregistration

1. HR department shall mail copy of release order to IT team as and when required basis, informing about employees who have been released on transferred to other dept./Site/unit/ superannuated/terminated from employment.
2. The IT team shall deactivate user id or change the password/forward the mails to defined user-id within 8 hours after receiving the information from HR.
3. When user-id is deactivated, files associated with the user-id shall be deleted unless a specific request is received from respective user’s department for transferring the files to another user-id or archiving the files to tape.
4. IT team shall maintain the records of user-id deregistered for 6 months.
5. IT team shall maintain the records of user-ids, which need to be continued on special ground.
6. User e mail id deregistration will also be done thru intimation of reporting manager of employee.

# Backup Operation

The frequency of the backup is on daily incremental and weekly full basis.

* The full backup of the TFS Servers is scheduled for every day, and DC weekly. External mass storage is used for taking the back up of TFS and DC.
* Azure - Backup of machines snapshots retention is 3 days
* Azure - MS SQL database backup retention is 7 days

In case of finance backup, one copy is available on external mass storage and second copy is available on one drive

# Backup Media Labeling

The media will be labeled as DDMMYYYY, along with daily/weekly/monthly tag and the type of data/server.

# Backup Recovery & Testing

1. System Administrator shall do the restore verification check of backup media once in a month on a random basis. Every month, the selection of backup tapes shall be done from different backup scheme (daily, weekly, monthly) and different partitions. System Administrator shall record the tapes verified. The records shall be maintained for 1 year.
2. Backup recovery from tapes on user’s request shall be done only after receiving the user’s request on prescribed form “Form for File Recovery from Backup” available on Intranet site. The records of request form shall be maintained for 1 year.

# Backup Media Management

1. The latest version of backup (monthly, weekly backups) tapes shall be stored off-site
2. The backup tapes shall be packed in a sealed case for off-site. Authorized person shall do the seal on the packed backup tapes.
3. Authorized person shall record the offsite movement of backup tapes. The records of tape movement shall be maintained for 1 year.

# First-Aid & Fire-Fighting Practices

1. Fire extinguishers shall be kept at various places in the Server Room. Smoke detectors and heat detectors shall be installed in the Server Room and around. The fire extinguishers shall be checked every quarter and the smoke and heat detectors shall be checked every year by concerned department. Employees shall be trained to use the fire extinguishing equipment.
2. First-aid box shall be kept in the premises equipped with the bandages and the required medicines.

# Internet Infrastructure

The Internet infrastructure includes leased line modems, routers, switches, and necessary servers to run required services.

1. Required modems, routers and other equipment shall be kept in a secured room.
2. Power to this rack shall be provided through UPS.
3. Regular monitoring shall be done for availability of Internet and its required services like DNS servers, web servers, proxy servers and mail servers. Log shall be maintained for availability of services.
4. If any of the services becomes unavailable, then operator shall inform the network administrator immediately.

# 12.1 Procedure to Check Internet Services

Authorized person shall check & take corrective actions on receipt of complaint from users.

# Network Infrastructure

The network infrastructure includes switches, hubs, routers, leased line modems and necessary servers to run required services.

1. Documentation shall be maintained for all inventory including network rack locations, switches, IP addresses, network points etc.
2. All racks shall be locked, and authorized person should maintain keys.
3. Power to all switches shall be provided through UPS.
4. Regular monitoring shall be done for availability of network at all locations. Log shall be maintained for availability of network.
5. External agencies within NST India Limited shall be provided restricted network access.
6. Preventive maintenance shall be done for all racks once a year.

**13.1 Procedure to Check Network Infrastructure**

1. Network administrator shall check the network using scripts.
2. Result shall be logged and action on any adverse report shall be taken. If at any time, a user complains about non-working of network, Network administrator shall find out the problem and take corrective action.

**13.2 Procedure to maintain network devices (Firewalls, routers, and Switches)**

1. Operational rules in firewall will be applied only after approval of network administrator.
2. Regular backup of configuration of network devices will be taken at defined frequency (presently at weekly interval and as and when changes take place)
3. Whenever there is change in configuration of network devices the existing configuration will be archived and new configuration is tested before deploying in the production environment.

# Monitoring System & Use

1. System Administrator shall daily monitor the critical server and its logs to ensure the availability and integrity of server.
2. Any unusual activity or unusual messages in the log files like unauthorized access, server fault, system crash etc. shall be recorded along with clear description and time.
3. The unusual activity/fault should be analyzed, and corrective action taken should be recorded.
4. System Administrator shall maintain the log files and logbook records for 3 months.
5. Time adjustment of all servers (i.e., clock synchronization) shall be done automatically from a timeserver during off hours (6:00PM to 6:00AM) or on holidays.

# Software Media Management

1. All software media received, shall be marked with unique code number according to coding scheme and shall be logged.
2. Server software shall not be issued to any other person apart from system administrator.
3. Copies of all other software shall be made and only copied software shall be issued to anyone. Register shall be maintained for issue and receipt.
4. All software media shall be stored in locked Almirah and keys shall be controlled by IT in charge.

# E-Mail System

1. Network Administrator will put limit on size of incoming and outgoing mail messages for employees is (which is 10 MB), for functional head is (which is 20 MB) and for IT admin is (which is 50 MB). Exceptions for management

Following types of attachments are blocked on Mail Serve/IMSS server:

.bat ,.chm,.com,.cpl,.dll,.dot,.exe,.hta,.js,.lnk,.ocx,.pif,.dcr,.shr,.vbe, .vbs, .wsf

1. System Administrator shall put email address or source IP address in the email deny list, which are found sending spam, virus, or objectionable mails.
2. System Administrator shall keep the virus identity data on Mail server updated.
3. System Administrator shall maintain the message log files for 6 months.
4. System Administrator shall develop the System utilities for day to day operations like backup utility to manage backup operation

# Publicly Available Information

***Internet Web Site***

1. Admin rights of NST website are with IT department.
2. System Administrator shall ensure the availability of the Web Server including periodic maintenance of server & checking of links.
3. System Administrator shall keep current security patches, evaluate, and expeditiously apply as appropriate.
4. System Administrator shall properly restrict access to information and maintain a log and monitor the access to Web Server at regular intervals.
5. Editing rights to website are available with authorized list of personnel in marketing department. Editing of content to website is done as per NST documentation standards.
6. Hosting of website will be done by third party under monitoring of Data Center.
7. No individual / Section shall host a web site/ web server of their own without information to & permission from web master. Defying policy will lead to disciplinary action.

# Privilege Management

There are special circumstances where extra or privileged access is needed. For all such cases, the information contained within an account or information pertaining to the activity of an account, is carefully restricted and must only be carried out with the appropriate authorization and safeguards in place.

1. Privilege allocation should be approved by IT Department Head and the role and need of privilege should be clearly defined.
2. System Administrator shall develop the System utilities for day-to-day operations like backup utility to manage backup operation.
3. System Administrator shall ensure the proper authorized access permission to system utilities.
4. System Administrator shall at least annually review the privileges and revoke the redundant privilege rights.
5. System Administrator shall maintain the privilege allocation and revocation records. Privilege revocation records shall be maintained for 6 months.

**Appendix A-** Access in special circumstances

|  |  |
| --- | --- |
| Special Circumstances | Detail |
| Information Security and System Administration | The Information Security team/SEPG Team may access accounts and user data. Some examples are;   * Business continuity. * To detect and prevent crime (including but not limited to, fraud and unauthorized access to computer systems). * System security protection: Virus, malware, hacking and other infected device and account prevention. * To establish the existence of facts relevant to the business of the institution (for example - where a case of suspected plagiarism is being investigated and there is sufficient evidence, the communications and/or files may be examined without prior user consent). * Misuse, abuse, and illegal activity investigation. |
| Regulatory Requests | A request for information to satisfy a regulatory request (e.g., Subject Access Request) can be made to the Information Security/SEPG team. Requests will be considered by the information system security committee as required. |
| Previous Account Owner | A request for information held against a previously active account by the account owner may be approved only after a careful review and on a case-by-case basis. Requests will be considered by the information system security committee as required. |
| Medically Incapacitated or Deceased User Account Access | Access requests can be made to the Information Security/SEPG team. Requests will be considered by the information system security committee as required. |

# Clock Synchronization

* Clock synchronization will be done.
* In case of unwarranted situation, clock synchronization can be done during shutdown or there may be cases when clock synchronization cannot be done due to database constraints the same will be identified as a risk in Risk Register.