

Antivirus Process

**Version History:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ver. | Date | Description of Change | Authored / Revised By | Reviewed By | Approved By |
| 1.0 | 21st, May 2008 | Initial Draft | Jyotsna Bareja | Abhishek Rautela | Mr. Sudhir Saxena |
| 2.0 | 16th Sep 2009 | The Symantec antivirus was removed and the policy was updated with the MacAfee antivirus. | Abhishek Rautela | Rohitash | Mr. Sudhir Saxena |
| 2.1 | 14th Oct 2011 | Update Antivirus EPO version and installed new features | Ausaf Khan | Dhananjay Kumar | GM Dua |
| 3.0 | 21st May 2012 | Update section Sec 3.0 &4.0 | Saket Madan | Dhananjay Kumar | GM Dua |
| 3.1 | 22nd Aug 2013 | Update section 3.0, 4.0 & 5.0 for ISMS purpose and change NST logo | Saket Madan | Dhananjay Kumar | Ajay Kumar Zalpuri |
| 3.2 | 3rd Dec 2018 | Update section 3.0 and 5.0 for Antivirus | Saket Madan | Dhananjay Kumar | Ajay Kumar Zalpuri |

Table of Contents

[1.0 Purpose 4](#_Toc369870128)

[2.0 Scope 4](#_Toc369870129)

[3.0 General Policy: 4](#_Toc369870130)

[4.0 Rules for Virus Prevention 5](#_Toc369870131)

[5.0 IT Department Responsibilities 6](#_Toc369870132)

[6.0 Individual Responsibilities: 6](#_Toc369870133)

[7.0 Enforcement: 6](#_Toc369870134)

# 1.0 Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to NST in terms of lost data, lost staff productivity, bad effect on hardware and/or lost reputation.

As a result, one of the goals of NST is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by NST employees to help achieve effective virus detection and prevention.

# 2.0 Scope

This policy applies to all computers that are connected to the NST network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both company-owned computers and personally-owned computers attached to the NST network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices, and servers.

# 3.0 General Policy:

1. Currently, NST is using a licensed Bit Defender. The most current available version of the anti-virus software package will be taken as the default standard.
2. The Bit Defender server is located at NST and all the computers are linked with server to receive updates.

3.   All computers attached to the NST network must have standard anti-virus software (Bit Defender) installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.

4.   Any activities with the intention to create and/or distribute malicious programs onto the NST network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly discouraged.

5.   If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the System department immediately.Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

6.  No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the system administrator.

7.   A virus-infected computer which is being noted repeatedly consecutively 3 times will be removed from the network until it is verified as virus-free.

8. To block all the social sites access, because by accessing these particular sites effecting (spreading virus) NST systems hardware, software.

9. The USB mass storage is blocked by NST.

#  4.0 Rules for Virus Prevention

1. The standard anti-virus software provided by NST shall automatically scan the systems as per the rule set by the administrator.
* Every day virus definition update
* Weekly full system scan

2.  Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3.   Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.

4.   Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

5. Files that shall be blocked by the e-mail system are decided by the System Administrator.

6. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

7.   Back up critical data and systems configurations on a regular basis and store backups in a safe place.

# 5.0 IT Department Responsibilities

The following activities are the responsibility of the NSTIT department:

1. The IT department is responsible for maintaining and updating this Anti-Virus Policy. This policy shall be available in the QMS.
2. The IT department will keep the anti-virus products up to date.
3. The IT department shall be responsible for installing anti-virus software on all NST owned and installed desktop workstations, laptops, and servers.
4. The IT department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.
5. Personally owned computers are managed by the gateway antivirus.
6. Weekly Scanning task schedule by Bit Defender, which is automated.
7. System generated report can be viewed or download through EPO console. The analysis will be done for infected machine an action will be recorded.

# 6.0 Individual Responsibilities:

The following activities are the responsibility of NST departments and employees:

1. All employees are responsible for taking reasonable measures to protect against virus infection.
2. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the NST network without the express consent of the IT department.

# 7.0 Enforcement:

This policy shall be implemented, administered and enforced by the IT Department.