# HPOL#14
# Virus and Malicious Software Protection

**(Version 1.0)**

# Table of Contents

## 14.1. SCOPE AND OBJECTIVES

Viruses and Malicious Software (Malware) are unauthorized programs that replicate themselves and spread to other computer systems across a network or through infected media such as floppy diskettes. The symptoms of Virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

Viruses and Malware are a potential risk to the confidentiality, integrity and availability of the government organization's Information Systems. This document relates to the government organization's policy for the prevention, detection and removal of Viruses and Malware.

## 14.2. POLICY STATEMENT

### 14.2.1. VIRUS AND MALWARE PROTECTION POLICY

#### 14.2.1.1. Prevention of Viruses and Malware

14.2.1.1.1. Virus and Malware detection infrastructure must be implemented at points where Viruses and Malware can be introduced into the government organization's network.

14.2.1.1.2. The government organization's process to update the Virus and Malware detection infrastructure with the latest product and Virus signature updates as soon as these updates are released must be implemented.

14.2.1.1.3. The installation of Virus and Malware protection software on any new potential point of entry (new Personal Computers, servers, etc.) of Viruses or Malware or to determine that the new (potential) point of entry is covered by an existing installation of such software must be in accordance with the government organization's defined procedures.

14.2.1.1.4. Procedures should exist to obtain and verify information regarding potential threats from malicious software and related hoaxes. This information is communicated to government organization staff, as required.

14.2.1.1.5. The steps/decisions to be taken to protect the government organization's Information System infrastructure from a new Virus or Malware - before the government organization's Virus and Malware protection infrastructure is updated to address the new risk, must be in accordance with the Virus and Malware Contingency Plan.

14.2.1.1.6. The government organization's process to ensure that Virus and Malware detection infrastructure remains active and is not disabled at any potential entry point must be implemented.

#### 14.2.1.2. Detection of Viruses and Malware

14.2.1.2.1. Memory resident components of Virus and Malware detection infrastructure in Personal Computers, servers,

laptop computers and other appropriate components of the government organization's information systems infrastructure should be implemented.

14.2.1.2.2. Anti-Virus software scans must be performed on all Personal Computers, servers, laptop computers and other components of the government organization's information systems architecture at periodic intervals to detect potential Viruses and Malware.

14.2.1.2.3. All files downloaded from the Internet or E-mail systems, or introduced via floppy disks or CD ROMs or through any other media or interconnection / networking facility must be scanned for Viruses and Malware.

14.2.1.2.4. The government organization's process must be implemented to update the Virus and Malware detection infrastructure with the latest product and Virus signature updates as soon as these updates are released.

14.2.1.2.5. The government organization's process must be implemented to install Virus and Malware protection software on any new components (new Personal Computers, servers, etc.) of the network or to determine that the new (potential) point of entry is covered by an existing installation of such software.

14.2.1.2.6. The steps /decisions to be taken in the event of the entry of a Virus into the government organization's information systems infrastructure must be in accordance with the Virus Malware Contingency Plan.

14.2.1.2.7. The government organization's process to ensure that Virus and Malware detection infrastructure remains active and is not disabled on any component of the government organization's information systems infrastructure, must be implemented.

**14.2.1.3. Removing Viruses and Malware**

14.2.1.3.1. The infected system must be immediately isolated from the network infrastructure and handled in accordance with the

Virus and Malware Contingency Plan.

14.2.1.3.2. The Virus must be removed using appropriate anti-Virus software.

14.2.1.3.3. Virus scans of all components of the Information Systems infrastructure must be conducted to detect any further cases of infection.

14.2.1.3.4. Designated personnel of the government organization must investigate the path used by the Virus to enter the network and appropriate prevention measures must be implemented to prevent recurrence.

#### 14.2.1.4. User Responsibilities

14.2.1.4.1. Users must be prohibited from changing the configuration of, removing, de-activation or otherwise tampering with any Virus and Malware prevention / detection software that has been installed on systems used by them.

14.2.1.4.2. Users must report all incidences of Virus (detected by the installed anti-Virus software) immediately to designated personnel of the government organization.

14.2.1.4.3. The infected system must be immediately isolated from the network infrastructure and handled in accordance with the Virus and Malware Contingency Plan.

14.2.1.4.4. It is the responsibility of users to ensure that all anti-Virus updates made available to them are immediately implemented on the workstations, desktops, laptops, and/or other equipment assigned to them.

14.2.1.4.5. Users must ensure that exchanges of media with other organizations are checked for Viruses and Malware.