

DOCUMENT: POLICY	DOCUMENT NUMBER: 0502	REVISION: ORIGINAL	PAGE OF 1 7
SUBJECT: VIRUS PREVENTION, DETECTION AND REMOVAL		EFFECTIVE DATE: September 6, 2000	
ORIGINATOR:	DATE:	OFFICE OF MIS:	DATE:
OPERS:	DATE:	SECRETARY OF DHHR:	DATE:

1.0 PURPOSE

The purpose of this policy is to (1) establish a procedure that defines the responsibilities for reducing the threat of computer viruses to computer resources within the Department of Health and Human Resources (DHHR); (2) to promote employee awareness of the threat posed by computer viruses; (3) to ensure that anti-virus software is properly installed and utilized on a regular basis; (4) to establish responsibility for overseeing computer virus prevention; and (5) to establish a reporting mechanism to ensure that all appropriate personnel are contacted in case of a computer virus incident.

2.0 SCOPE

This policy applies to all employees, personnel from other organizations, contracting personnel, and vendors using DHHR systems and participating in sponsored software development, software demonstrations, and the operation and maintenance of IT systems.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 ARTICLE 3C - WV Computer Crime and Abuse Act.
- 3.2 Policy 0501 Use of IT Resources

4.0 RESPONSIBILITY/REQUIREMENTS

Computer viruses come in two basic forms, destructive and non-destructive. Destructive viruses can damage or destroy data and programs. Non-destructive viruses display messages or some other form of non-destructive action. Detecting and removing even a non-destructive virus takes time and money. For this reason it is important that viruses are detected before an infection occurs, or at least as soon as possible to prevent it from spreading.

4.1 SOFTWARE ACQUISITION AND INSTALLATION

- 4.1.1 Employees will use only software furnished by DHHR. Under special circumstances, software may be used if it has been approved by the employee's immediate supervisor and the Network and Technical

DOCUMENT: Policy	DOCUMENT NUMBER: 0502	REVISION: Original	PAGE 2 OF 7
SUBJECT: Virus Prevention, Detection and Removal		EFFECTIVE DATE:	

Support (NTS) Group.

- 4.1.2 All software, data, and/or program files must be scanned for viruses before installation. In the case of software distributed in compressed form, scanning must be done immediately after installation.
- 4.1.3 Because shareware and freeware are often sold by individuals or by small companies whose reputations are not established, and because of the openness of the means used to distribute the software, special precautions must be taken before it is installed on DHHR computers. These precautions include:
- 4.1.3.1 Determining that the software does not "misbehave", interfere with, or damage agency hardware, software, or data.
 - 4.1.3.2 Determining that the software does not contain viruses either originating with the software designer or acquired in the process of distribution.
 - 4.1.3.3 Shareware or freeware will be obtained directly from its author or from a shareware company bulletin board dedicated to support the company's software.
 - 4.1.3.4 Shareware and other employee-procured software will not be installed or used unless approved by the employee's immediate supervisor and the NTS.

4.2 DHHR/OMIS RESPONSIBILITIES

- 4.2.1 The DHHR, Office of Management Information Services (OMIS) will evaluate, recommend, install, and maintain virus protection software and/or tools for use on any DHHR desktop computer and network servers.
- 4.2.1.1 The OMIS will enter information to schedule date, time and frequency of "live updates" provided by the vendor to the virus protection software.
- 4.2.2 Only software purchased or individually approved by DHHR management may be used or installed on a DHHR computer.

DOCUMENT: Policy	DOCUMENT NUMBER: 0502	REVISION: Original	PAGE 3 OF 7
SUBJECT: Virus Prevention, Detection and Removal		EFFECTIVE DATE:	

4.2.3 Virus protection software shall be loaded on each desktop computer and server(s) as a terminate and stay resident program to constantly monitor for viruses to prevent introduction to the network.

4.2.3.1 Data and program files that have been electronically transmitted (for example, E-Mail) to a DHHR computer from another location, internal or external, should be automatically scanned for viruses as they are being received. Be advised that some viruses may pass through undetected.

4.2.3.2 The Virus Coordinator receives virus alerts from the vendor providing anti-virus software.

4.2.3.3 When virus alerts are received, the Virus Coordinator will evaluate the information provided and determine proper virus alert disposition. Normally, the Virus Coordinator will disseminate the virus alert to the ISO, the Manager of the Network and Technical Support and other pertinent OMIS personnel. Recipients must acknowledge receipt of all virus alerts.

4.3 EMPLOYEE RESPONSIBILITIES

4.3.1 If you receive a message for a Live Update from the anti-virus software, you must choose the option "**Run the Event Now**". Do not cancel or delete the event.

4.3.2 OMIS is responsible for maintaining the virus protection system. While a virus should be blocked from entering your workstation, the system will inform you that your e-mail contained a virus. You are then responsible for informing the **sender** of the e-mail that their message contained a virus.

4.3.3 Most viruses come as attachments to e-mail. The attachment must be executed for the virus to infect your computer. **For this reason users are advised to NEVER execute programs or open attachments that (1) you have not requested, (2) that come from a person you do not know, or (3) that you have not scanned with current anti-virus software.**

4.4 VIRUS REPORTING BY EMPLOYEES

DOCUMENT: Policy	DOCUMENT NUMBER: 0502	REVISION: Original	PAGE 4 OF 7
SUBJECT: Virus Prevention, Detection and Removal		EFFECTIVE DATE:	

4.4.1 When the anti-virus software detects what appears to be a virus, the software will provide pertinent information about the virus and the employee will take the following actions:

- 4.4.1.1 Write down the name of the virus (if provided).
- 4.4.1.2 Write down any recent unusual system activities (for instance, unexpected disk access, error messages or screen displays) and/or affected files.
- 4.4.1.3 Immediately notify OMIS HELP DESK (558-9999) or your Equipment Coordinator, providing all pertinent information regarding the source of the virus.
- 4.4.1.4 Put a "Do not use" note on the PC.

4.5 OMIS VIRUS OVERSIGHT RESPONSIBILITIES

4.5.1 The NTS will investigate all reports of apparent computer virus infections and will oversee the effort to remove the virus from the affected computer.

4.5.2 The OMIS HELP DESK shall take the following steps:

- 4.5.2.1 Document the name of the virus if provided by the virus protection software.
- 4.5.2.2 Actively seek to identify and document any recent unusual system activities (for instance, abnormal system behavior, error messages or screen displays) and, if possible, include when these activities were first noticed.
- 4.5.2.3 Inform the user not to use the PC until the virus has been eradicated.
- 4.5.2.4 Assign the virus to a technician as "**Priority 1**", and inform them immediately by telephone, by page, or in person.

4.5.3 OMIS TECHNICIANS shall take the following actions:

DOCUMENT: Policy	DOCUMENT NUMBER: 0502	REVISION: Original	PAGE 5 OF 7
SUBJECT: Virus Prevention, Detection and Removal		EFFECTIVE DATE:	

- 4.5.3.1 Go to infected workstation, document the name of the virus and attempt to determine the source of the virus and the method of transmission.
 - 4.5.3.2 Take appropriate steps to eradicate the virus. These steps will vary depending on the virus.
 - 4.5.3.3 After repair steps have been taken, make sure the latest definitions are downloaded, re-scan the drives, and ensure that the appropriate settings are defined to allow updates to be kept current.
 - 4.5.3.4 The technician will enter all pertinent information into the Help Desk system and will provide the ISO with a service report (call ticket) stating what the virus was and a brief explanation of the solution.
 - 4.5.3.5 If the technician is unable to correct the virus problem within one hour, he/she will promptly notify the immediate supervisor for further direction.
 - 4.5.3.6 If the technician suspects that a DHHR system user has intentionally initiated or distributed a virus onto a DHHR computer, or if it appears that malicious code was written specifically for a DHHR system, the ISO and the NTS manager will be notified immediately.
- 4.6 Monthly Virus Reporting
- 4.6.1 The OMIS Help Desk will generate, through the Help Desk system, a monthly report which includes information pertaining to the number of viruses detected. This report will be forwarded to the ISO by the 10th of the following month.
- 4.7 OMIS ISO VIRUS INVESTIGATION RESPONSIBILITIES
- 4.7.1 The Information Security Officer (ISO) is the person designated by the CIO to monitor and provide initial enforcement of DHHR's information security program and IT policies.
 - 4.7.2 The Secretary of the DHHR has designated the Office of the Inspector General (OIG) as the primary authority to investigate any reported instances of departmental employee misconduct.

DOCUMENT: Policy	DOCUMENT NUMBER: 0502	REVISION: Original	PAGE 6 OF 7
SUBJECT: Virus Prevention, Detection and Removal		EFFECTIVE DATE:	

4.7.3 The ISO may investigate any report of an apparent computer virus infection, and will, in certain cases, make an effort to investigate the source or carrier of the infection. The ISO will keep the CIO and other personnel (OIG) as necessary, advised of the findings of the investigation.

4.8 VIOLATIONS AND DISCIPLINARY ACTION(S)

4.8.1 No employee will deliberately introduce a virus into DHHR computer(s) or withhold information necessary for effective virus control procedures. All suspected violations of this policy shall be reported to a supervisor in the chain of command above the employee.

4.8.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to his/her Office Director or Bureau Commissioner for appropriate action.

4.8.3 After reviewing all allegations, the Bureau Commissioners may refer the alleged abuse or misconduct to the ISO and/or the OIG as warranted for further investigation.

4.8.4 Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to: (1) progressive disciplinary action as outlined in DHHR Policy 2104; or (2) criminal prosecution. Levels of discipline include:

- Verbal reprimand
- Written reprimand
- Suspension
- Demotion
- Dismissal

5.0 DEFINITION OF TERMS

Introduction of viruses and other malicious software programs has generated a whole set of new terms. The following list of definitions is provided to familiarize personnel with some of these terms.

5.1 Chief Information Officer (CIO) is the director of OMIS and the person responsible for all information resources within the DHHR.

DOCUMENT: Policy	DOCUMENT NUMBER: 0502	REVISION: Original	PAGE 7 OF 7
SUBJECT: Virus Prevention, Detection and Removal		EFFECTIVE DATE:	

- 5.2 Information Security Officer (ISO) is the person designated by the CIO to establish and administer DHHR's information security program.
- 5.3. Virus Coordinator - Person designated by the CIO to monitor and coordinate anti-virus activities within the DHHR.
- 5.4 PC - A personal computer that may also be called a workstation.
- 5.5 LAN - A group of PC's connected to one another
- 5.6 Virus detection software - Software written to scan machine-readable media on computer systems. There are a growing number of reputable software packages available that are designed to detect and/or remove viruses. In addition, many utility programs can search text files for virus signatures or potentially unsafe practices.
- 5.7 Scan -To examine computer coding/programs sequentially, part by part. For viruses, scans are made for virus signatures or potentially unsafe practices. (e.g., changes to an executable file, direct writes to specific disk sectors, et al.).
- 5.8 Computer virus - A program that "infects" computer systems in much the same way as a biological virus infects humans. The typical virus reproduces by making copies of itself and inserting them into other programs-either in systems software or in application programs.