1.0 PURPOSE

The purpose of anti-virus software is to provide the Department of Health and Human Resources (DHHR) with comprehensive protection against computer viruses and malicious code. This protection includes the tools and procedures necessary to prevent major and widespread damage to user applications, files, and hardware. In addition to protecting the information on individual workstations and servers, anti-virus software protects the DHHR network. The availability, performance, and security of the network are essential to the daily operation of the Department. Viruses and other forms of malicious code (worms, Trojans, backdoors, VBS scripts, mass-mailers, etc.) represent a significant threat to this operation.

2.0 SCOPE

This policy applies to all employees using DHHR systems and participating in sponsored software development, software demonstrations, and the operation and maintenance of Information Technology (IT) systems.

3.0 APPLICABLE DOCUMENTS/MATERIAL

3.1   Chapter 61, Article 3C – WV Computer Crime and Abuse Act

3.2   DHHR IT Policy 0501 – Use of IT Resources

3.3   DHHR IT Policy 0510 – E-mail Guidelines and Requirements

3.4   Office of Management Information Services (OMIS) Operating Procedure 06 – Virus Reporting

3.5   DHHR Policy Memorandum 2104 – Progressive Discipline

3.6   DHHR Policy Memorandum 2108 – Employee Conduct

4.0 RESPONSIBILITY/REQUIREMENTS

4.1   DHHR/OMIS Responsibilities

4.1.1   OMIS will evaluate, install, and maintain anti-virus software and/or tools for use on all DHHR desktop computers, laptops, servers, and other computing devices.

4.1.1.1   All software **must** be installed by OMIS technicians.

4.1.1.2   Employees will only use software furnished by the DHHR. Under certain circumstances, software may be used if it has been approved by the employee's immediate supervisor, the Network and Technical Support (NTS) group, and/or the Data Center Desktop Support (DCDS) group.

4.1.2   All workstations and servers connected to DHHR computer network resources must have OMIS supported anti-virus software correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network.

4.1.2.1   Data and program files that have been electronically transmitted to a DHHR computer from another location, whether internal or external, should be automatically scanned for viruses as they are being received.

4.2   Anti-Virus Coordinator Responsibilities (see OP-06)

4.2.1   The OMIS Anti-Virus Coordinator will ensure that a reliable process is in place to receive notification from anti-virus software vendors of new virus threats, as well as monitor the DHHR network for virus incidents.

4.3   Employee Responsibilities (see OP-06)

4.4   Monthly Virus Reporting

4.4.1   The OMIS Help Desk software will generate a monthly report, which includes information pertaining to the number of viruses detected. This is included in the NTS and DCDS management report sent to the Chief Technology Officer (CTO).

4.5   Enforcement Authority

4.5.1   The ISO has been designated by the CTO to monitor and provide initial enforcement of the DHHR Information Security program and IT policies.

4.5.2   The ISO may investigate any report of an apparent computer infection; and will, in certain cases, make an effort to investigate the source or carrier of the infection. As necessary, the ISO will keep the CTO and other relevant personnel advised as to the findings of the investigation.

4.6 Violations and Disciplinary Action(s)

4.6.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.6.2 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 the Office Director of Bureau Commissioner for appropriate action.

4.6.3 As determined by the Office Director or the Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.6.4 Employees who willfully or knowingly violate or otherwise abuse the provisions the provisions of this policy may be subject to: (1) disciplinary action as outlined in DHHR policy 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

5.1 Anti-Virus Coordinator – The person designated by the CTO to monitor and coordinate anti-virus activities within the DHHR.

5.2 Bureau Commissioners – Senior leaders who report directly to the Secretary of the DHHR and manage the various Bureaus of DHHR, (i.e., the OIG, and the Bureaus for Public Health, Children and Families, Behavioral Health and Health Facilities, Child Support Enforcement, and Medical Services).

5.3 Chief Technology Officer (CTO) - The director of OMIS and the person responsible for all information resources within the DHHR.

5.4 Computer Virus – Software used to infect a computer with a destructive program.

5.5 Data Center Desktop Support (DCDS) – The OMIS organization that is responsible for the DHHR Data Center and the Kanawha County offices.

5.6 Employee – Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractors' employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this policy. For the purposes of this policy, this also refers to anyone using a computer connected to the DHHR network.

5.7 Network and Technical Support (NTS) - OMIS unit that provides both first and second level support to all computer and network employees in the DHHR field offices.

5.8　Office of the Inspector General (OIG) – The office designated by the Secretary of the DHHR to investigate and/or assist in investigating allegations of employee abuses or misconduct.

5.9　Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.

5.10　PC – A personal computer; also called a workstation.

5.11　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.).

5.12　Virus Detection Software – Software that defends a PC against viruses and other malicious Internet code by scanning incoming attachments in e-mail and from other programs.