ANTIVIRUS

ISSP-14-0410

1. **SUBJECT:** Standard software and procedures must be implemented to minimize the impact of computer viruses on OPIC's information resources.
2. **SCOPE:** This policy applies to all OPIC servers and workstations, as well as any computers used for remote access to the OPIC network. Exceptions may be granted for operating systems that do not have readily available virus detection software.
3. **DESCRIPTION:** Computer viruses are programs that reproduce themselves and often attempt to do harm to the computers that they infect. Viruses may destroy OPIC data, make OPIC computers unusable, use OPIC's computer to attack other computers, or perform a variety of other malicious activities. There are many different types of computer viruses.

   Use of antivirus software is essential for protecting OPIC resources from the danger posed by computer viruses and other malicious programs. These programs check for viruses on OPIC's computers and attempt to remove them before they can spread or perform further damage.

   However, antivirus programs take time to learn about each new virus that is created, during which the virus can do serious damage. Therefore, it is also important that users and system administrators be aware of the risks posed by viruses, and take steps to minimize exposure to them.

4. **PROCEDURES & GUIDELINES:**

   (a) Every OPIC server and workstation must run the agency standard, supported antivirus software.

   (b) OPIC will use antivirus software at its email gateway to scan messages and attachments.

   (c) Employees may not unload or disable antivirus software for any reason without specific instruction from IRM.

   (d) Antivirus software is to be updated automatically as new virus profiles are made available by the vendor.

   (e) Any computer used for remote access to the OPIC network (such as a laptop used for telecommuting or a home computer used to do OPIC work) must have approved antivirus software loaded and updated on a regular basis.

   (f) Any infected files that cannot be repaired must be quarantined or deleted.

   (g) Any infected computers that cannot be cleaned by the antivirus software must be removed from the network until they can be verified as virus free.

   (h) Employees are to be trained on techniques for avoiding viruses, including the following guidance:

(1) Never open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and empty your Trash.

(2) Delete spam, chain, and other junk email without forwarding.

(3) Never download files from unknown or suspicious sources.

(4) Never install any software on OPIC computers without specific permission from IRM.

(i) All portable media (*e.g.* floppy diskettes, CDs) must be scanned for viruses before use on an OPIC computer.

(j) If lab testing conflicts with antivirus software, run the antivirus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the antivirus software. When the antivirus software is disabled, do not run any applications that could transfer a virus, *e.g.*, email or file sharing.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for deploying antivirus software and procedures on any servers or workstations that they own.

(b) Information Custodians are responsible for assisting information owners with the implementation of antivirus software and procedures.

(c) Information Users are responsible for taking appropriate precautions to avoid introducing viruses into the OPIC computing environment.

(d) Supervisors are responsible for assisting their employees with understanding and complying with OPIC antivirus procedures and guidelines.

(e) The Information Systems Security Officer (ISSO) is responsible for:

(1) Auditing the OPIC computer environment for adherence to this policy.

(2) Ensuring all personnel are trained on the application of this policy.

6. **DEFINITIONS:**

(a) Antivirus software– commercially available software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus may have caused.

(b) Remote Access – Any access to OPIC's corporate network through a network, device, or medium that is not controlled by OPIC (such as the Internet, public phone line, wireless carrier, or other connectivity).

(c) Virus – A malicious program which, when executed, copies itself onto other media or files available to the computer executing it and may cause damage to a computer system by attacking or attaching itself to boot information, email, data file, or another program.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)
9. **ATTACHMENTS:** None
10. **AUTHORITY:**

(a) OPIC Directive 00-01, Information Systems Security Program.

(b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

(c) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(d) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(e) Homeand Security Presidential Directive / HSPD-7, December 17, 2003

(f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

11. **LOCATION:** TBD
12. **EFFECTIVE DATE:** October 22, 2004
13. **REVISION HISTORY:** None
14. **REVIEW SCHEDULE:** This policy should be reviewed and updated annually.