DEPARTMENT OF HUMAN GENETICS 01-02

CATEGORY: SUPPORT SERVICES
SECTION: Computing, Information, and Data
SUBJECT: Antivirus Policy
EFFECTIVE DATE: March 27, 2013 Revised
PAGE(S): 2

I. SCOPE

This policy is designed to help prevent infection of Department computers and computer systems by computer viruses and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

This policy applies to all employees and faculty of the Department; as well as vendors, contractors, partners, students, collaborators and any others doing business or research with the Department will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving Department computers and technology systems will also be subject to the provisions of this policy. Every user of Department computer resources is expected to know and follow this policy.

II. DEFINITIONS

Computer devices are any type of device connected to a network that could become infected with a computer virus. Examples of computer devices would be, but are not limited to, workstations, servers, laptops, etc.

Malicious software is any type of computer code that infects a machine and performs a malicious action. This is sometimes perpetrated by computer viruses, worms, trojans, etc.

Anti-Virus software runs on either a server or workstation and monitors network connections looking for malicious software. Anti-virus software is generally reactive, meaning a signature file must be developed for each new virus discovered and these virus definition files must be sent to the software in order for the software to find the malicious code.

Virus definition files are periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software.

III. POLICY

Server

1. All Department of Human Genetics servers shall have anti-virus software installed and configured so that the virus definition files are current, routinely and automatically updated, and the anti-virus software must be actively running on these devices.

2. The anti-virus software will report its findings to an internal anti-virus server.
3. All files on the server will be scanned periodically for viruses.
4. If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected server may be disconnected from the network until the infection has been removed.

Workstation

1. All Department of Human Genetics computer devices connected to the network shall have anti-virus software installed and configured so that the virus definition files are current, routinely and automatically updated, and the anti-virus software must be actively running on these devices.
2. The anti-virus software will report its findings to an internal anti-virus server. This is required to help ensure the safety and security of the Department network.
3. All files on computer devices will be scanned periodically for viruses.
4. If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the network until the infection has been removed.

Exceptions to this policy may be allowed if a computer device cannot have anti-virus software installed. Possible examples of this would be vendor-controlled systems, or devices where anti-virus software has not yet been developed.

This policy will not supersede any University of Pittsburgh developed policies but may introduce more stringent requirements than the University policy.