DEPARTMENT OF HUMAN GENETICS 01-07

CATEGORY:	SUPPORT SERVICES
SECTION:	Computing, Information, and Data
SUBJECT:	Intrusion Prevention Policy
EFFECTIVE DATE:	April 19, 2013 Revised
PAGE(S):	2

I. SCOPE

This policy is designed to help prevent unauthorized access of Department computers and computer systems by outside network access. This policy is intended to help prevent unauthorized usage of user applications, data, files, and systems.

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 potentially be accessed from outside of the Department for malicious purposes. Examples of computer devices would be, but not limited to, workstations, servers, laptops, etc.

Compromised computers could be used to find confidential information or be used to attack other systems.

Anti-Virus software runs on either a server or workstation and monitors the network for malicious connections. Logs files for authentication and system functions can also show the presence of unauthorized access.

III. POLICY

Server

1. All Department of Human Genetics servers shall have their logs monitored for any suspicious activity on a weekly basis. This may be done by either an IT Department member or by software designed to monitor and alert on any unusual changes.
2. Any suspicious entries found will be immediately dealt with. This could include blocking the suspicious IP address to taking the server offline if needed.

Workstation

1. All Department of Human Genetics computer devices connected to the network shall routinely have their logs monitored for any suspicious activity. This may be done by either an IT Department member or by software designed to monitor and alert on any unusual changes.
2. The anti-virus software may report its network threat protection logs to an internal anti-virus server. This is required to help ensure the safety and security of the Department network.
3. If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, a compromised device may be disconnected from the network.

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