DEPARTMENT OF HUMAN GENETICS 01-05

CATEGORY: SUPPORT SERVICES
SECTION: Computing, Information, and Data
SUBJECT: Microsoft Computer Security Policy
EFFECTIVE DATE: April 15, 2013 Revised
PAGE(S): 1

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 Microsoft Windows laptop and desktop computer users. Every user of Department computer resources is expected to know and follow this policy.

III. POLICY

1. Users are required to change their password once every six months. Users who login using their Pitt IDs will have this enforced automatically via Pitt's policies. However, those who log onto their computers using local accounts will be required to manually change their passwords.
2. Microsoft Update should be configured to automatically check for updates. Users who log into their computers using their Pitt ID will have this configured automatically. Those who log into their computers using a local account will need to verify that their computer has the most recent updates from Microsoft at least once a month.
3. Antivirus software and anti-malware software will be installed and running on the system. Refer to Antivirus Policy 01-03 for further information.
4. Users that will keep confidential data on their laptops will be required to install Computrace on their system and possibly encrypt the data. Refer to Confidential Data Policy 01-08 for further information regarding confidential data.

Any questions about how to configure their computer to meet this policy should contact the Human Genetics IT Help Desk.

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