**DEPARTMENT OF HUMAN GENETICS 01-06**

|  |  |
|---|---|
| **CATEGORY:** | SUPPORT SERVICES |
| **SECTION:** | Computing, Information, and Data |
| **SUBJECT:** | Lab Computer Security |
| **EFFECTIVE DATE:** | March 4, 2014 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. Also, this policy is to help reduce the chance of theft of Department data.

This policy applies to all lab computer users. Every user of Department lab computer resources is expected to know and follow this policy.

## III. POLICY

1. All computers are required to have a security lock installed to help prevent physical theft. This includes any data drives that are attached to the computer.
2. All users are required to use their own Pitt login or a shared Pitt resource account.
3. All lab computers will automatically lock after 15 minutes of inactivity.
4. Protected Health Information (PHI) or HIPAA data may not be stored on removable drives, such as an external hard drive or USB memory stick. All identifiable data should be stored on a predetermined Department file server.
5. All lab computers will meet the security standards set by Pitt. This includes complex and changing passwords.

Any questions about 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.