IT Security Policy

- Anti-Virus and Software Updates

Anti-virus software must be installed on all laboratory computers that are connected to our network. Recommended anti-virus software is distributed under Yale University's site license agreement. Laboratory employees are required to keep their computer's anti-virus software and operating system software up to date. When prompted to perform operating system or anti-virus updates you must comply within a reasonable amount of time in order to keep our network safe. If you need assistance in scheduling updates on your computer please contact us. Your computer should be checking for updates daily.

- Password security recommendations

Keep your passwords private. Do not share them with *anyone* including your supervisor, family, co-workers, or IT support provider.

1. Change any weak default passwords for local applications so that they employ strong passwords.
2. Change your passwords periodically.
3. If your password is discovered or you determine that someone is using it to access your account, contact the System Administrator.

- Portable Computing Devices

Portable computers offer staff the ability to be more productive while on the move. They offer greater flexibility in where and when staff can work and access information, including information on our Laboratory's network. However, network-enabled portable computers also pose the risk of data theft and unauthorized access to our network.

Any device that can access the network must be considered part of that network and therefore subject to policies intended to protect the network from harm. Any portable computer that is proposed for network connection must be approved and certified by the IT department.

a) Protecting your Laptop

In order to qualify for access to our Laboratory's network, the laptop must meet the following conditions:

1. Network settings, including settings for our VPN, must be reviewed and approved by IT support personnel.
2. A personal firewall must be installed on the computer and must always be active.

3. Anti-virus software must be installed. Software must have active scanning and be kept up-to-date.

b) Laptop User's Responsibilities

1. The user of the laptop is responsible for network security of the laptop whether they are onsite, at home, or on the road.

2. The user of the laptop is responsible for keeping their operating system and anti-virus software up-to-date at all times. It is strongly recommended that they update their anti-virus software and any critical operating system patches before going on the road.

3. The user of the laptop shall access network resources via a VPN connection. Use of public Internet services is discouraged, as they do not offer adequate protection for the user.

▪ Avoid activities that may compromise security

When using a web browser, be aware that the less you know about a site, the greater the dangers. For secure sites (sites whose address begins with "https" instead of "http") examine the web address carefully to assure it is as expected. Always examine embedded links to see that they point to an address consistent with what you expect. If any question, type in the expected address manually rather than follow a programmed link.

Be very careful when installing any program on your computer. Many programs that can be downloaded from the Web automatically install spyware or other malicious software ("malware") on your computer. Only download software from well-known software vendors.

▪ Electronic Protected Health Information (ePHI)

The Federal Department of Health and Human Services (HHS) implemented the Privacy Rule which provides standard secure computing guidelines for utilizing, storing and transmitting Protected Health Information (ePHI). The Privacy Rule helps organizations comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Pierce Laboratory computers, data storage devices, portable computing devices, and networks are not required to comply with these secure data protection guidelines since the organization's research and business activities do not collect, maintain, utilize, store or transmit and individually identifiable personal health information.

For more information regarding the Pierce Laboratory's formal policy on ePHI please see: *POLICY ON THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR RESEARCH PURPOSES.*