Technical Support Services

Personally Owned Computer Equipment Policy

Introduction

The Technical Support Services department of The John B. Pierce Laboratory, Inc. provides computer and information systems support for all staff members. In this document *Technical Support Services*, *IT Department*, and *IT* are all synonymous. Personally-owned computers are often used by laboratory employees to perform their lab-related work.

Purpose

The purpose of this policy is to:

- Ensure that Lab data are adequately protected
- Minimize the personal liability of staff in the event of a data loss
- Clarify support responsibilities for personally-owned equipment

What is Personally Owned Computer Equipment?

Personally owned computer equipment is any computer related device that was not purchased with John B. Pierce Laboratory funds.

Policy

Due to limited resources, the IT support staff is unable to provide general hardware and software support for personally-owned computing equipment, regardless of the physical location of that equipment.

Employees should not connect any personally owned computing devices to laboratory computers or network devices unless expressly permitted to do so by the IT support staff. Prior to granting network access the IT staff will install proper anti-virus protection and screen the computer for malware and known problem software (i.e. peer-to-peer file sharing software). Once network access has been granted personally-owned computers may be brought into the Laboratory and connected to the network for the purpose of conducting laboratory-related work.

Employees should follow all Laboratory computer usage policies when operating personally-owned computing equipment during work hours, on work premises, or while connected to the laboratory network.

In accordance with Lab data security policies and for personal liability purposes, staff should not make copies of Lab data to be edited or accessed on non-Laboratory equipment. The IT department is not responsible for backing up critical laboratory data stored on personally-owned computing equipment.

Staff working remotely or working from home should connect only to password protected, encrypted networks. When remotely connecting to the Pierce Lab network we require the use of VPN or SSH. See IT staff for VPN or SSH client installation and configuration.

Technical Support Services

In the event that your personal computer becomes infected, the computer must be cleaned before it is put back on the Laboratory network. Any known infections must be reported to IT staff prior to attempting connection to our network. IT staff will then attempt to disinfect your computer and may recommend a complete reinstall of the operating system to guarantee the infection is eradicated.

The use of unsecure portable USB storage devices is not recommended for laboratory data. The IT department will provide you with secure portable USB storage devices for lab-related work.

Data Loss Disclosure

Any loss or theft of a personally-owned computing device containing Laboratory data must be immediately reported to the IT Department. Any loss or theft of <u>any laboratory-owned computing device</u> must be immediately reported to the IT Department.