Personal Data Privacy Statement

Introduction

The John B. Pierce Laboratory takes reasonable steps to protect any personal data and to protect such information from loss, misuse, and unauthorized access, disclosure, alteration, or destruction.

Internet Security

Data transmission across the Internet is subject to normal internet security risks. As noted, no Internet or e-mail transmission is ever fully secure or error free. In particular, e-mail sent to or from the Laboratory's mail server is not secure, and you should therefore take special care in deciding what information you send or request be sent to you. Please keep this in mind when disclosing any personal data to any party via the Internet. Moreover, when you use passwords, ID numbers, or other special access features at the Laboratory, it is your responsibility to safeguard them.

Our internal network is protected by a firewall which prevents unauthorized access to our servers and all desktop computers from the internet.

Our email server maintains real-time updates of its anti-virus and anti-spam filters. Virus' and spam are common methods by which intrusions occur and private data is misused by outside data miners.

We operate a Windows Update Server which schedules and tracks Windows operating system updates and vulnerabilities.

We do support several methods of secure data transmission upon request. Our firewall allows VPN (Virtual Private Networking) in which remote computers can securely access internal computers and resources. This connection requires a username and password and all transmissions are encrypted. Also in use at the Laboratory is SSL (Secure Socket Layer) and SFTP (Secure File Transfer Protocol). Refer to our *Remote Connection Information* page on the IT Support Services website.

Portable computers, cell phones, handheld organizers, and portable data storage devices offer staff the ability to be more productive while on the move. They are also a privacy and security challenge for businesses and IT departments across the globe. At this time we only provide minimal protection in the form of anti-virus software for portable computers. We also suggest that you enable the Windows firewall when using your portable computer outside the laboratory's firewall. Refer to our *Laptop Security Policy* located on the IT Support Services website for more information.

Physical Security

Our company servers are located in a physically secure area accessible only by authorized personnel. The servers are stored in locked server racks. The console interface to the servers requires special keyboard codes for the system to become accessible and then each server requires an administrator password to log on.

Our data backup media is located in the locked server cabinets and in locked fireproof vaults in the shop supervisor's office. Backup data is also stored offsite in a secure location.