



## *Technical Support Services*

# **Network Security Policy for Portable Computers**

---

## Introduction

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.

## Protecting the 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. Recommended firewall software is Zone Labs' ZoneAlert or MS Windows XP Pro SP2.
3. Anti-virus software must be installed. Software must have active scanning and be kept up-to-date. Recommended anti-virus software is Symantec Antivirus distributed under Yale University's site license agreement.

## 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 anti-virus scanning software up-to-date at all times. It is strongly recommended that they update their anti-virus software 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.