INFORMATION SECURITY GUIDELINE

Firewalls

Introduction

1. This guideline is meant to provide guidance on configuring firewalls to protect UBC Electronic Information.

2. This guideline has been issued by the Chief Information Officer to supplement the Securing Computing and Mobile Storage Devices/Media standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

3. Properly configured firewalls provide an additional layer of defense that works with anti-virus and regular patching, in the overall protection of UBC Systems and UBC Electronic Information. The focus of this guideline is primarily host based firewalls; it should be noted if a network based firewall is required for a department or faculty, UBC IT provides a Virtual Firewall Service.

Firewall Instructions

Operating System	Instructions
Windows	Windows 7: http://windows.microsoft.com/en-ca/windows/understanding-firewall-settings#1TC=windows-7 Understanding Windows Firewall Settings: http://technet.microsoft.com/en-us/network/bb545423.aspx Getting Started Guide (Vista, 7, 2008 Server 2008R2 Server): http://technet.microsoft.com/en-us/library/cc748991%28v=ws.10%29.aspx
Apple - Mac OSX v 10.5, 10.6:	http://support.apple.com/kb/ht1810
Apple - OS X Mavericks:	Set firewall access for services and apps: http://support.apple.com/kb/PH14191 Prevent unwanted connections with a firewall: http://support.apple.com/kb/PH14267?viewlocale=en_US

Related Documents

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems
Securing Computing and Mobile Storage Devices/Media standard