Server Security Policy

1.0 Overview

Server computers contain confidential and personal information. Because the University takes compliance seriously, a variety of steps will be taken to ensure the security of this data. This policy outlines the steps that must be taken.

2.0 Purpose

This policy is designed to provide specific guidelines that must be followed by OIT system administrators to ensure the integrity of their servers and the data contained therein.

3.0 Scope

This policy impacts OIT staff members who are responsible for the day-to-day system administration tasks for a server that houses University data. Non-OIT staff members who maintain servers are strongly encouraged to follow the steps outlined herein.

4.0 Policy

OIT system administrators must take a number of steps to ensure the security of University data.

1. *Firewalls* - All production systems shall be protected by a software firewall to prevent access to services which should not be available to the general public. Information classified as Clarkson Confidential shall be protected by a hardware firewall.
2. *Patch Management* - All production systems shall be additionally protected by being kept up-to-date with the latest patches that are available for the software installed on them. This prevents an attacker from exploiting a known vulnerability.
3. *Anti-Virus Software* - All Windows based servers shall run anti-virus software to prevent a network-based virus from penetrating the firewall and infecting the machine. This anti-virus software shall be kept up to date with the latest virus definitions. If an automatic updating process is used to update the virus definitions, it should be checked on a daily basis to ensure proper operation.
4. *Account Management* - All systems containing user accounts shall be maintained in such a way as to ensure that users who are no longer affiliated with the University are denied access. When an individual leaves the University, his or her access should be removed as prescribed in the Account Deactivation Policy.
5. *Log Retention* - All systems should maintain detailed logs that should be rotated on an appropriate basis. In addition to keeping logs on the local machine, logs should also be sent via the network to a centralized log collection facility (ie. netmon) where they can be monitored and analyzed by the Network Engineer or the Manager of Network Operations. All logs should be kept for a minimum of six months, unless otherwise required by law or policy.

5.0 Enforcement

6.0 Definitions