Policy No: 815
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Server Registration Procedure

BACKGROUND

Information accessible through the Internet is available worldwide. Unfortunately, the incidence of hacking attempts continues to grow. Although the greatest threat is from locations off campus, inappropriate access to servers is possible from any computer on campus as well. The result of unauthorized access to a server can result in major financial penalties, legal action, business disruption and damage to the university's image. This overview is supplemental to and does not supersede the official CSU Policies for Connecting Devices to the University Network.

In order to protect the CSU network from unwanted intrusions, the University utilizes a firewall on the connection to the external Internet. The firewall is used to manage all outbound traffic from the CSU network to hosts on the Internet. Incoming connections to machines on the CSU network will be blocked unless registered with the University's Division of Information Technology & Services (ITS)

POLICY

In order to protect University resources, all servers must be registered with the Division of Information Technology & Services (ITS). Registration provides information necessary to monitor these resources and help protect them from intrusion.

To submit an application for a server to be registered on the CSU network a CSU Server Registration Application form must be completed. One application should be completed and submitted for each machine that is connected to the CSU network. If you have questions or require assistance in completing this form, please contact the Serve Help Desk or put in a SysAid service order ticket.

Administrators should exercise caution when determining which services to activate. Only those services absolutely necessary should be enabled on any machine. Services are defined as protocols such as, but not limited to, FTP (used for file transfer) and HTTP (used for the web) that run on the servers connected to the CSU network.

The registered administrator's responsibilities include, but are not limited to, physical security of the machine, applying all security patches immediately as they become available and reporting any suspected breach of security to the Chief Information Officer (CIO). All administrators are responsible for complying with the CSU Policies for Connecting Devices to the University Network and monitoring the CSU Server Administrator email list. The University reserves the right to deny any requests for connectivity to the network and/or access through the firewall. In accordance with the CSU Incident Response Plan, a security incident involving a particular server or servers, access to those machines may be blocked until the situation is resolved.

If the registration application has been approved, a passive port scan will be conducted and all requirements for tightening the security on the machine will be reviewed with the systems administrator. Should highly vulnerable ports be found, IT staff may, with or without notice to the system administrator, remove access to the vulnerable server until such time as the machine is no longer a risk to CSU or internet systems.