California State University Northridge	**Information Technology** Registration of Internet Devices	**Page** 1 of 2	
		SOP#: 500-03	**Revision#:**

Prepared by: Unknown **Date:** October, 18, 2004	**Approved by:** Previously approved by President as policy 500-03 **Date:** October 18, 2004
Last revised by: Chris Olsen, ISO **Date:** November 7, 2011	**Last approved by:** Chris Olsen, ISO **Date:** November 7, 2011

1.0 INTRODUCTION

Any computer, server, printer, or network-attached device that is located on campus and is directly accessible from off-campus locations requires special access through the campus firewall. Such special access introduces a vulnerability to the campus computing infrastructure.

To manage this vulnerability, all such devices must be identified and appropriate controls enabled. These controls will help to ensure that the services provided by an identified device, the device itself, and the campus computing infrastructure maintains a high level of confidentiality, integrity and availability.

Such controls are necessary to reduce the campus's vulnerability to electronic attacks, which could result in loss of university data and loss of access to services.

2.0 PROCEDURES

Each device that is directly accessible from off-campus locations must be registered with Information Technology (IT). The following procedures are associated with the registration of these devices.

1. The organizational administrator (e.g., Director, MAR, Dean, etc.) responsible for the device must submit a request to the University Helpdesk. This request must contain the following information:

    - The contact information for the organizational administrator
    - The 24x7 contact information for both the primary and secondary technical
    - The list of ports that need to be accessible from off-campus locations (refer to http://www.iana.org/protocols/ for assigned port numbers) A general description of the unique services being provided by this device, including the following information:

- The DNS name and IP address for the device: (A DNS name and static IP address must also be associated with this device.)
- The physical location of the device
- The services (or applications) that are offered via this device
- The community served by these services
- The reasons why existing Internet services currently do not meet the needs in which this device would provide.

2. The security department will conduct a vulnerability scan of the device or application to identify vulnerabilities. The device owner will then fix the vulnerabilities.
3. Following a successful vulnerability scan, the Information Security Officer (or designee) shall review and approve the firewall opening request.
4. IT will make appropriate configuration changes to the campus firewall in accordance with Change Management procedures.
5. A yearly review of all registered devices and associated firewall rules will be conducted.

3.0 APPLICABILITY AND AREAS OF RESPONSIBILITY

1. The technical administrators are responsible for keeping IT informed of the status of their Internet Service Devices. In addition, these devices must conform with campus policy and adhere to prevailing IT standards.
2. IT must assist campus entities with their requests for expanded data communication needs.
3. IT/NEO is responsible for all configuration and maintenance of the firewall devices.
4. The technical administrators are responsible for fixing vulnerabilities on internet accessible devices.

4.0 RESOURCES AND REFERENCE MATERIALS

State Administrative Manual (SAM), Section 8643

500-8045 Network Security and Security of Devices Connecting to the Network