California State University Northridge	**Information Technology** Network Hardware Standard	**Page** 1 of 2	
		SOP#: 500-06	**Revision#:**

Prepared by: Unknown **Date:** October 18, 2004	**Approved by:** Previously approved by President as policy 500-06 **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

All network communications devices, including but not limited to, hubs, mini-hubs, port splitters, bridges, routers, switches or wireless access points cannot be connected to the campus network without prior authorization from IT. Any unauthorized network device or any network device that may be negatively impacting the management or the quality of service of the campus network may be disconnected by IT.

The campus network is a resource used by the entire campus community. To ensure that this resource is properly maintained and available for its intended use, all network hardware must conform to a minimum, uniform standard.

Monitoring and troubleshooting is more complex when such devices share the same physical port, adding cost, delay in problem resolution and potential performance loss. Improperly configured network devices may also pose a substantial security risk. This policy is not meant to completely prohibit the use of these devices, but to ensure that the most appropriate solution for the campus and individual application is used.

2.0 PROCEDURES

- Upon detection and confirmation that a device is adversely affecting the integrity of the campus network,
    - IT will notify the responsible technical contact (when possible) that the device is to be disconnected from the network.
    - IT shall disable the port serving the device and take other protective steps as deemed appropriate.
- The device shall remain disconnected from the network until the device no longer negatively impacts the Campus computing environment.
- IT will assist the affected entity to specify and install either permanent or temporary additional connections as required.

- Network devices, such as hubs, mini-hubs, port splitters, bridges, routers, and switches, or wireless access points may be approved for temporary connection to the campus network under the following conditions:

  - The use is for a specific project and time period, after which the device will be removed.
  - The device will only be used in a specific location and not moved without prior authorization.
  - The device must be manageable (as appropriate) by either IT or by an entity authorized by IT.
  - Any network problem caused by such an unauthorized device, or by attached device(s), will result in the disconnection of the unauthorized device.
  - The entity installing the device is responsible for all maintenance and troubleshooting for the device.

3.0 APPLICABILITY AND AREAS OF RESPONSIBILITY

The Chief Information Officer (CIO), will work with the Sr. Director of Infrastructure Services to ensure that the minimum University standard for networking equipment confirms to prevailing technology, industry best practices, and CSU Guidelines, and for ensuring that these standards meet the needs of the Campus.

Campus system administrators (desktops or servers) are responsible for keeping IT informed of their network connection needs. System administrators are responsible for all network devices not acquired in coordination with IT, including any devices attached to them. All such devices must be secured with appropriate passwords and configured to minimize security and performance risks to the campus network. IT must assist campus entities with their requests for additional connectivity and ensure the proper functioning of ports provided as a result.

4.0 RESOURCES AND REFERENCE MATERIALS

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