USA Network Connection Policy

I. Purpose of This Policy

The University networks support a wide variety of devices and services of critical importance to the operations of the University. In addition to providing University constituents access to electronic mail, Internet, and file and print services, the networks also support telephony, monitoring of environmental control and other equipment, remote security monitoring, and other essential University services.

The connection by individuals of equipment which is not appropriately designed and configured for the corporate network not only can disrupt network services and create avenues for security breaches, but in fact, has happened at the University.

The Computer Services Center is charged with the design and operation of the University networks.

II. General Rules

With the exception of the Permitted Devices enumerated below, no device may be connected to the University network, and no wireless connection devices may be activated within University building spaces, without the ***PRIOR WRITTEN*** approval of the Computer Services Center.

III. Permitted Devices

1. Personal computers (desktop, laptop, notebook, etc.) and Personal Digital Assistants ("smart phones") may be attached directly to network wall connections or joined to the University 802.11 wireless network. This is the case whether the device is owned by the University, a University constituent, or vendor performing work for the University. The Computer Services Center reserves the right to access and configure any device directly connected to the University wired network.
2. Bluetooth devices connected to personal computers, such as keyboard, mouse, etc. (Permission does not constitute a guarantee of support for these devices from the Computer Center).
3. Networked printers may also be directly connected to the University network connections, but individuals are advised to contact the Computer Services Center for assistance to ensure correct configuration for operation on the University networks.

   NOTE: Users are not to configure static IP addresses on such devices except as provided by the Computer Center.

IV. Prohibited Devices and Actions

All other devices require the written approval of the Computer Services Center before connection. You are advised to consult with the Center before acquiring such equipment, as approval may not be granted.

a. Switches, routers, hubs, splitters, or any other device which is inserted between the network connection and the personal computer .
b. Moving or connecting campus-provided networked (VOIP) telephones to different network jacks, except under the explicit instruction of Telecommunications or the Computer Services Center.
c. Connection of any wireless access points to the University network, or the installation and operation of any independent 802.11 wireless access point within University buildings.
d. The use of personal computers or PDAs to provide downstream network connections to other devices, whether wired or 802.11 wireless.
e. Configuring network services or server functions on their personal computer, such as DHCP or bridging/routing services, which would disrupt network connectivity for other users.

V. Authorization of Computer

The introduction of a computer device, including a personal computer, which will be used as a server to provide resources to other computers on the University networks. The Computer Services Center will provide consultative services for departments considering acquiring servers.

VI. No Delegation of Authority

Various technical support groups within the University, including the Health Systems Information Services group, college and departmental IT technical staff, provide essential support to the operations of the University. They may assist end users with acquiring permission, but they themselves must acquire the written approval of the Computer Services Center, and are not authorized by the Center to grant any approval of network connections as described in this document.

VII. Removal of non-approved or disruptive equipment

Computer Services Center staff will remove any non-approved equipment or equipment causing disruptions of network services. If such equipment is determined by the Computer Center to pose an intrinsic risk to the University networks, the Computer Center may arrange for the disposal of this equipment. If the equipment is

not University owned, the Computer Center will consult with the Vice President of the academic or administrative unit of the employee as to the proper disposal of the equipment.