

## **University Local Area Network Connection Policy**

**3/2/2007**

The Christopher Newport University data network is a vital shared resource used by the entire campus. The data network provides access to all on-campus and Internet-based resources. The connection of network devices to the CNU network impacts the overall network performance. The intent of this policy is to define procedures that ensure safe, secure, and reliable network resources are available to all campus departments.

### **Policy**

All network devices must be approved prior to their introduction on the CNU network. A “network device” is defined as any hardware component that communicates via the CNU local area network. “Approval” consists of an official written acknowledgement by IT Services indicating the specific network device and citing the agreed upon purpose.

Examples of network devices:

- Printers
- Desktops
- Laptops
- Hubs
- Switches
- Routers (wireless and wired)
- Firewalls

Network devices which change the network topology of the CNU network are not permitted. This policy applies to all segments of the CNU network, including the Residential Network, Administrative Network, and the Wireless Network.

### **Residential Computing**

All residential student computers are subject to register on the CNU Residential Network and to pass a “security state” inspection. The security inspection verifies that student computers have:

- a. The latest Operating System updates
- b. An up-to-date version of the CNU Anti-Virus software.

Until a student computer has been registered and passed the security inspection, the student computer will only be able access limited Internet-based resources and all on-campus publicly accessible resources. Once a student computer has been registered on the CNU Residential Network, it will be allowed full access to off-campus Internet resources.

### **Administrative Computing**

All administrative desktop and laptop computers are subject to this policy and must be registered with CNU IT Services. Registration ensures that the computer is running the CNU mandated Anti-Virus and an up-to-date Operating System. Laptops and desktops that are setup and deployed by IT Services with the CNU system image are automatically approved to connect to the network.

**Additional Wired Network Capacity**

If additional port capacity is required for an on-campus wired installation, an IT Services Helpdesk request must be submitted. The associated costs for this installation will be billed to the requesting department.

**Wireless Guest Computing**

Guests on the CNU campus can obtain limited Internet access by associating with the CNU-Guest wireless network, available in the University Library and the David Student Union. Guest access is offered without any expectation of privacy or safety and is available at the risk of the guest. The CNU-Guest network requires that the user be re-authenticated after 30 minutes of usage.

**Non-University Owned Devices Attached to the CNU Network**

Network devices which belong to faculty, staff, or students, including laptops, desktops, and network printers must be approved before connecting to the CNU production network. These machines are subject to the same rules about security as all other machines on the network.

**Request for Network Communications Device Approval**

Name:

Department:

Phone:

E-mail:

Manufacturer:

URL:

Model:

URL:

Description of device:

Description of need for device:

\*\*\* Please attach network diagrams and/or equipment specifications as appropriate. \*\*\*

Requested: \_\_\_\_\_

By: \_\_\_\_\_

Date

Signature – Requestor \*

\* By signing this request, I acknowledge that I have read and understand the Network Connection Policy.

Approved \_\_\_\_\_ By: \_\_\_\_\_  
Date Signature – Network Manager

Rejected

Stipulations: