Policies of the University of North Texas	Chapter 14
14.004 Network Connections	**Information Technology**

Policy Statement. UNT's data communications network is a critical resource shared by all campus units: it provides the means to communicate both within the University and via the Internet to the rest of the world. The introduction of communications devices that might affect the behavior or performance of the network without proper planning for security and performance requirements has the potential of resulting in disruption of services to everyone on campus. Similarly, the addition of high-bandwidth servers to the network can degrade the performance of every device on UNT's internal network. This policy is intended to define a procedure that insures secure, reliable, and sufficient network capacity to all campus units through a review of communications devices and high-bandwidth servers prior to their deployment on UNT's network.

Application of Policy. Total University

Definitions. None

Procedures and Responsibilities.

I. The addition of devices that could conflict with other approved devices on the network, or of devices that place high demands on network bandwidth, must be approved prior to their introduction. “Devices” are defined as hardware components or software services running on common desktop or server machines that communicate over UNT's local area network. The following examples of types of devices would require approval:

   A. Multicasting
   B. Services that answer broadcast messages, such as DHCP and BOOTP
   C. Devices that answer ARP requests as servers (such as security tools and network management tools)
   D. Firewalls that operate at a level higher than a single machine in the network hierarchy
   E. Routers
   F. Bridges
   G. Switches
   H. Proxy servers
   I. Wireless access points
   J. High bandwidth devices (averaging more than 1 GB/day for a week)
   K. (Other similar devices also require approval: this list is not comprehensive)

   A department planning to add a device or service that alters the topology of the network or places high demands on network bandwidth must submit a Remedy

request for approval to add the device/service, using a Remedy form that is designed for that type of request.

The Director of Communications Services will expeditiously review the request and reply to the Remedy request, possibly with stipulations about how the addition must be configured. If the request is approved, the communications device or service may be added to the network as approved, in accordance with UNT's Computer Use Policy (policy 14.003) and UNT's Information Resources Security Policy (policy 14.002.) However, if it is subsequently determined that the communication device/service is causing disruptions to other users or compromising the security of the network, the device will be removed from the network by the data communications department or by the network manager responsible for the device. The Director of Communications Services will then review the issue with the user department to determine an appropriate course of action.

Responsible Party: Director of Communications Services

II. Personally-Owned Devices Attached To The Network. Personally-owned devices such as laptop computers owned by faculty, staff, or students may be attached to the network if a departmental network manager agrees to allow such personally owned machines to be attached to the subnetwork for which the network manager has responsibility. However, if the personally-owned device falls under the provisions of the above restrictions governing machines or services that alter the topology of the network, the network manager must first request permission from the Director of Communications Services to attach such device/service to the network. A written request to attach personal machines must be submitted to the network manager (the form for such requests follows) and the network manager must sign the form indicating approval before the machine may be added to the network. Those machines are subject to the same rules about security and bandwidth conservation as all other machines on the network.

Responsible Party: Departmental Network Manager

III. Wireless Access Points and Devices. Wireless access points are specifically listed above as devices that affect the topology of the network. Such devices have the potential of allowing unauthorized users to consume bandwidth and of opening the network to security breaches. Therefore, no wireless access point may be added to the network without prior authorization as noted above.

The data communications department employs technologies and network configurations to protect the campus network and systems from unauthorized access via wireless connections. Wirelessly-connected devices such as laptops or personal digital assistants are allowed to connect to the campus network through an authentication mechanism that requires a UNT login account or a temporary account that is specifically granted to the persons using the devices.

Network managers and persons with a need to assign temporary wireless access may authorize persons to attach to UNT's wireless network. The Director of

Communications Services grants rights to network managers and others upon a request with a justified need for those rights.

Responsible Party: Departmental Network managers; Director of Communications Services

IV. Removal of Malfunctioning Devices from the Network. At all times, the security, reliability, and performance of the network are important to the accomplishment of the University's mission. Therefore, if any device on the network is found to compromise any aspect of the network's operation, the data communications department, in coordination with the network manager with responsibility for the subnet on which the device is attached, may summarily remove the device from the network. The user and user's department will be informed when that action is taken and the data communications department will work with the affected department to bring the device up to accepted standards of operation.

Responsible Party: Departmental Network Manager

V. Appeals. If a request to deploy a communications device or service is denied, the requestor may appeal the decision to the Associate Vice President for Computing and Chief Technology Officer. The Associate Vice President for Computing and Chief Technology Officer may seek the recommendation of the Communications Planning Group (CPG) of the Information Resources Council and may either consult with the department representatives and the Director of Communications Services and/or his designee(s) directly or ask the CPG to do so.

If a request to attach a personally-owned device to the network is denied by the network manager, the requester may appeal the decision to the Dean or Vice President with responsibility for the network manager.

Responsible Party: Associate VP for Computing and Chief Technology Officer; Communications Planning Group of the Information Resources Council; Director of Communications Services or his designee

References and Cross-references.

UNT Policy 14.003, Computer Use
UNT Policy 14.002, Information Resources Security

Approved: 8/1/2004
Effective:
Revised: 7/2011*
*Format only