Connecting Devices to the University Network

Information/Background:

The University at Albany communications network is a community resource and a foundation of the campus information technology infrastructure. The purpose of the network is to enable open, yet secure, transmission of information among its users and to the world beyond via the Internet.

The physical network consists of a cable and wiring infrastructure extending to most campus buildings, and on to each communications network jack. This cable plant is enhanced by the deployment of networking equipment in the form of routers, switches, and wireless access points. Network access is extended to a number of off-campus locations and rented facilities. The campus network maintains connections to the Internet and Internet2 and administers the class B domain address space of 169.226.

Access to the network is made possible through the connection of devices (personal computers, servers, etc.) via a wired (network jack) or wireless access point. Access to the network is available to all students and employees of the University and to a wide variety of affiliated organizations and individuals.

The purpose of this policy is to:

- identify those responsible for the network
- provide a framework for the ongoing development of the physical network infrastructure
- establish standards for the connection of devices to the campus network
- create linkage with, and support, the University's Responsible Use of Information Technology and Information Security Policies.

Policy Statement:

The University provides an integrated, robust, secure and reliable network infrastructure, consistent with available resources, to all authorized members of the campus community. Standards for physical network architecture and infrastructure development (network wiring, equipment, etc.) shall be developed and maintained, and shall have status equivalent to "building code." Additions and/or modifications to the network infrastructure, both wired and wireless, shall conform to these standards and are made by authorized staff only. Access to and modifications (installations, repair, and maintenance) of equipment in communications rooms are strictly limited to authorized personnel only.

The connection of devices to the campus network, whether by wired or wireless means, shall also be governed by standards and guidelines. These standards shall encompass security and technical requirements that protect the network as a community resource and promote ease of access and sharing of information resources. All devices connected to the University network must conform to the prescribed standards. The connection of devices to the network not meeting such standards is strictly prohibited.

The University shall administer and maintain the class B 169.226 domain in accordance with the terms and conditions of its assignment.

Network access is available to all authorized users with appropriate authentication. Network use is subject to the terms and conditions of the University's Information Security Policy.

Users shall utilize the network in support of their individual teaching, learning, and research goals, and job responsibilities.

Responsibility and Authority:

The responsibility and authority for the implementation of this policy, including the development, promulgation and implementation of the aforementioned standards and guidelines is vested in the Office of the Chief Information Officer (CIO). The Office of the CIO shall also be responsible for the allocation and maintenance of the University's class B 169.226 domain. This may be delegated.

All users and organizational units of the University and its affiliated organizations are responsible for compliance with this policy, and its applicable standards, guidelines and procedures. See also the Responsible Use of Information Technology Policy.

Rationale:

The University's mission is served by ensuring a stable, secure and robust network infrastructure. In order to provide consistent, stable and secure network services to all users, the University needs to have appropriate controls over the allocation of network resources. It also needs to protect the physical assets of the network infrastructure. Units wishing to modify network access in their area may do so under the auspices of the Office of the CIO and the Office of Network Services to ensure conformity with standards.
Companion Documents:
Standards for Connecting Devices to the University Network
Standards for Connecting Servers to the University Network
Infrastructure and Design Standards
Network Equipment Standards
Class B Domain Space Standards
Wireless Standards

Need more help? Contact the ITS Service Desk.