

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

<p><b>Network Security</b></p>	<p><b>6-005 INFORMATION TECHNOLOGIES July 2009</b></p>
--------------------------------	--

INTRODUCTION

- 1.01 The network of Oklahoma State University Institute of Technology exists to facilitate the research, education, and outreach missions of the University. The network provides electronic capabilities that allow University faculty, staff, students, or affiliates to access information, share data, collaborate, and communicate. Computer & Information Services (CIS) manages the network and is responsible for its secure and effective operation. CIS is responsible for the maintenance, planning and implementation of network growth and to coordinate these efforts with units and departments.

SCOPE

- 2.01 This policy is applicable to all individuals using University owned or controlled computer and computer communication facilities or equipment. It is applicable to all University information resources whether individually controlled or shared, stand alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the University. In addition, a user must be specifically authorized to use a particular computing or network resource by the campus unit responsible for operating the resource.
- 2.02 Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall Policy but may provide additional detail, guidelines and/or restrictions. Such policies may not relax or subtract from this policy. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for securing appropriate authorization and to furnish Computer & Information Services (CIS) with a copy of the approved document. Units must also publicize both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. In such cases, the unit leader shall provide the Executive Vice President with a copy of such supplementary policies prior to implementation thereof. Where use of external networks is involved, policies governing such use also are applicable and must be followed.

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY NETWORK  
COMPONENTS

3.01 The network consists of the following:

- A. Access-Layer Network Infrastructure - Network wiring and electronics (network switches and/or hubs) in University buildings that interconnect University computers and other devices.
- B. Wireless Network Access "Air Space" - Radio spectrum used for wireless network access at the University.
- C. Network Backbone and Building Switches - Top-level network switches/routers in each building and the core network backbone that connects University building networks together and to off-campus networks.
- D. Wide Area Network Connections - Wide Area Network (WAN) that connects distributed portions of the University network.
- E. Connections to Regional and National Networks (OneNet) - Off-campus connections to the Internet. OneNet is Oklahoma's telecommunications and information network for education and government. OneNet is a division of the Oklahoma State Regents for Higher Education and is operated in cooperation with the Oklahoma Office of State Finance.
- F. Core Network Services - Services required for network operations (Domain Name Service, boot P, Wins, etc.)
- G. Oklahoma State University Institute of Technology Network – The infrastructure to provide data and communication services and resources.
- H. Subordinate Departmental Network – An independent network whose development has been reviewed by CIS and approved by the Executive Vice President.

GENERAL PROVISIONS

4.01 Oklahoma State University Institute of Technology Network as a Principal Institutional System

The network is a critical campus principal institutional system, available to all faculty, staff, students or affiliates, at all campus locations. It provides end-to-end "wall plate to wall plate" service from any computer on campus to any other, as well as to off-campus computers and resources.

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

4.02 Subordinate Departmental Network

A departmental network is considered an independent system and shall not be directly interfaced with any institutional system. Any deviation to this must be reviewed by CIS and approved by the Executive Vice President.

4.03 Wireless Network

Wireless services are subject to the same rules and policies that govern other Information Technology at the University (examples include: Appropriate Use Policy, Use of Electronic Mail, World Wide Web Publishing Policy).

- Wireless equipment and users must follow general wireless communication protocols.
- Wireless access will be provided for public access in some public areas, such as the Library.
- Communication links will not be encrypted and will be restricted to selective services.
- All other wireless access will be limited to authorized faculty, staff, students and affiliates.
- Users will be required to authenticate before any connection will be allowed. Logs of all access and authorizations should be kept for a period of 90 days.
- Standard wireless encryption is to be used on all devices as appropriate.
- Anti-Virus Software is to be used on all devices as appropriate.
- All wireless needs should be directed to CIS for review and coordination.

4.04 Extension of the Backbone into New Buildings

The extension of the network into new buildings on campus should be included and funded as part of building construction projects. Buildings should not be erected without the capability to communicate with the University network or without CIS approval or blueprints and CIS involvement during construction. Installation of any communications wiring and/or facilities shall be performed in accordance to industry standards and requirements set forth by CIS.

4.05 TCP/IP – Oklahoma State University Institute of Technology 's Network Protocol

To facilitate interoperability among University systems, the network backbone supports only TCP/IP and other IP based protocols.

4.06 Involuntary Disconnection

To assure the integrity of the network, it may be necessary for CIS to disconnect a host, a group of hosts, or a network that is unsecured or disrupting network service to others. This includes hosts involved in network security problems, such as those used by unauthorized parties to attack other systems on the University network or on the Internet. If the situation allows, CIS will make an attempt to contact the local network administrator or owner of the host or hosts involved. If those individuals are not available, the disconnection may proceed without notification. With regard to security issues, a disconnection might be a "partial" one that isolates the host from attacking hosts, or from off-campus access in general. A host that has been compromised by

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

unauthorized parties may need to stay disconnected until the host's operating system can be updated and all changes made by the attacker reversed.

4.07 Physical Access to Wiring Closets

Only CIS is authorized to place equipment or cabling in wiring closets, equipment rooms, etc., unless special arrangements are made with CIS. At no time shall any individual access CIS wiring closets or shall any wiring not belonging to CIS be located within a CIS wiring closet without approval from CIS.

4.08 Exceptions to Interim Network Policy Requirements and Guidelines

Requests for an exception to a requirement or guideline of this policy should be directed to CIS for coordination and approval.

4.09 Mediation

If mediation is required, issues will be presented to an appropriate advisory committee for review. All decisions will be communicated in writing and will include justification for the decision.

COMPUTER AND INFORMATION SERVICES RESPONSIBILITIES

5.01 Network Maintenance

CIS maintains building and campus network wiring and fiber, local switches, building routers/switches, backbone routers/switches, and other network devices that comprise the University network. This includes troubleshooting problems, identifying their cause, and replacing or repairing defective equipment and wiring.

5.02 Network Documentation

CIS is responsible for creating and maintaining the detailed documentation of the network required for proper network maintenance, operation, and planning.

5.03 Administration of University Network Connections to Other Networks

CIS maintains relationships and agreements with OneNet and other service providers to keep the University network well connected to the commercial Internet. CIS administers all interfaces between networks and connections between the University network and other networks.

5.04 Administration of University Network Name and Address Space

CIS manages the University network name space and the assignment of names and network addresses (IP numbers) for security and identity of users.

5.05 Administration of University Wireless Networking

CIS coordinates use of wireless networking at the University to ensure compatible access to all University users.

5.06 Central Network Services

CIS provides central services required for operation of the network.

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

5.07 Network Devices

The network is a mission critical strategic University resource. In order to protect the Data Communications Network, devices other than computers, servers, and workstations must not be plugged into any network port. This includes, but is not limited to hubs, switches, repeaters, routers, network modems and wireless access points. These devices may be incorrectly configured or incompatible with the University network causing outages and reliability problems to all or part of the network. Devices not approved for use on the University's Data Communications Network will be disabled to ensure the stability and availability of the network.

5.08 Traffic Monitoring

CIS monitors traffic flow to optimize network usage, detect network problems, and ensure equitable access and other properly authorized investigations.

5.09 Security Monitoring

To the extent possible, CIS monitors incoming network traffic to detect the "signatures" of known network intrusion scenarios, viruses, or the like. CIS may periodically scan the University network hosts to assess the vulnerability to attack. It should be noted that there is no guarantee that CIS will be able to detect all potential system vulnerabilities.

5.10 Campus-Wide Network Security Coordination

CIS promotes campus-wide network security and coordinates campus-wide response to unauthorized access. This also includes working with local supporters, computer users, and OneNet to protect the campus from network intrusions, denial of service attacks, and other unauthorized and/or inappropriate activities that impair network access and use.

5.11 Planning for Network Growth

CIS interacts with campus units to ensure current and future communication needs are addressed.

5.12 Upgrades to Current Infrastructure

CIS performs upgrades to the current infrastructure to ensure current and future needs are addressed.

NETWORK ADMINISTRATOR

6.01 Oklahoma State University Institute of Technology's Network Administrator shall be the primary contact to work in conjunction with appropriate university officials for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. Any issues concerning law shall be referred to OSU Legal Counsel for advice and action as applicable.

6.02 In situations that are an immediate threat to the security or operation of a computer or network, the Network Administrator may require immediate intervention of access privileges and affected user files or messages. In such an emergency, the Network Administrator will notify, as soon as possible, the appropriate university administrators and users affected by the situation.

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

USER RESPONSIBILITIES

- 7.01 The owners or primary users of computers connected to the University network are responsible for the following:
- A. Abiding by Oklahoma State University Institute of Technology's Appropriate Computer Use Policy  
Users should efficiently use network resources and follow Oklahoma State University Institute of Technology's "Appropriate Computer Use" policy and Oklahoma State University Institute of Technology's "Network Security" policy. Users are personally responsible for all activities on their User ID or computer system and may be subject to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control, even if not personally engaged in by the person controlling the computer or system.
  - B. Reporting Problems  
Users should promptly report network problems to either the Network Administrator or to the CIS HelpDesk, and cooperate with support technicians in correcting malfunctions.
  - C. Taking Proper Security Precautions  
Users should select secure passwords and change them regularly. Security-minded network access techniques should be used whenever practical.
  - D. Keeping the Operating System Secure  
Users should make sure their computer's operating system is kept up-to-date with current security patches. This may be accomplished by the owner or local support technicians.

SPECIAL NOTIFICATIONS

- 8.01 Oklahoma State University Institute of Technology's computing and network systems are a University owned resource and business tool only to be used by authorized individuals for business and academic purposes. Users should never distribute mailing lists owned by the University. The University owns everything stored in its systems unless it has agreed otherwise. The University has the right of access to the contents of stored computing information at any time for any purpose for which it has a legitimate "need to know". The University will make reasonable efforts to maintain the confidentiality of computing information storage contents and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents. Devices not approved for use on the University's Data Communications Network will be disabled to ensure the stability and availability of the network.

NOTIFICATION

OKLAHOMA STATE UNIVERSITY INSTITUTE OF TECHNOLOGY  
POLICY & PROCEDURES LETTER

- 9.01 References to this policy will be on the Oklahoma State University Institute of Technology web site and in the Oklahoma State University Institute of Technology's Policies and Procedures manual.

APPLICATION AND ENFORCEMENT

- 10.01 Each University unit shall be responsible for enforcing this policy in a manner best suited to its own organization and in ensuring cooperation and coordination with CIS.