Network Security	6-005 TECHNOLOGY SERVICES December 2019

INTRODUCTION

1.01 OSU Institute of Technology (OSUIT)'s network exists to facilitate the education, research, administration, communication, and outreach missions of the university. The network provides electronic capabilities that allow university faculty, staff, students, or affiliates to access information, share data, store data, collaborate, and communicate. Technology Services (TS) manages the network and is responsible for its secure and effective operation. TS is responsible for the maintenance, planning, monitoring, and implementation of network growth and to coordinate these efforts with units.

SCOPE

2.01 This policy is applicable to all individuals using university owned or controlled computer and network 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 leader responsible for 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 TS 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. Where use of external networks is involved, policies governing such use also are applicable and must be followed.

OSUIT NETWORK COMPONENTS

3.01 The network consists of the following:

A. Access-Layer Network Infrastructure - Network wiring and electronics (network switches and wireless access points) in university buildings that interconnect university computers and other devices.

B. Wireless Network Access - Radio spectrum used for wireless network access at the university.

C. Network Backbone and Building Switches - Top-level network switches and 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 (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.

F. Core Network Services - Services required for network operations (Domain Name Service (DNS), boot P, Wins, DHCP, etc.)

G. OSUIT Network – The infrastructure to provide data, communication services, and resources.

H. Subordinate Departmental Network – An independent network whose development has been reviewed by TS and approved by the Associate Vice President of Technology Services.

GENERAL PROVISIONS

4.01 OSUIT Network as a Mission Critical System

The network is a critical principal institutional system, available to all faculty, staff, students, or affiliates at all campus locations. It provides end-to-end service from any computer or Internet enabled device on campus to any other authorized device, as well as to the Internet.

4.02 Subordinate Departmental Network

A departmental network is considered an independent system and shall not be directly interfaced with any institutional system.

4.03 Wireless Network

Wireless services are subject to the same rules and policies that govern other information technology at the university.

- Wireless equipment and users must follow general wireless communication protocols.
- Wireless access will be provided to authorized faculty, staff, students, and affiliates.
- Users will be required to authenticate through O-Key before any connection will be allowed.
- Employees can call the TS service desk to request a temporary service account for guest log on. Employee making the request is responsible for restricting the log on to identifiable persons for auditing purposes.
- Logs of all access and authorizations should be kept for a period of 90 days.
- Strongest available wireless encryption is to be used on all devices.
- Anti-Malware Software must be used on all devices.
- SPI firewall must be configured in deny all mode.
- All wireless needs should be directed to TS service desk for review and coordination.
- All users of the OSUIT network or computers must comply with the security policies mandated by the state of Oklahoma at https://www.ok.gov/OSF/documents/StateOfOklahomaInfoSecPPG_osf_12012008.pdf.

4.04 Extension of the Backbone into New Buildings

The extension of the network into new buildings on campus must 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 TS approval of IT related aspects of the blueprints and TS involvement during construction. Installation of any communications wiring and/or facilities shall be performed in accordance to industry standards and requirements set forth by TS.

4.05 TCP/IP – OSUIT '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 confidentiality, integrity, and availability of the network, it may be necessary for TS to disconnect a host, a group of hosts, or a network that is unsecured or disrupting network service to others. If the situation allows, TS will make an attempt to contact the owner of the host or hosts involved. If those individuals are not available, the

disconnection may proceed without notification. A host that has been compromised may need to stay disconnected until the host's operating system has been reinstalled.

4.07 Physical Access to Wiring Closets

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

4.08 Exceptions to Network Policy Requirements and Guidelines

Requests for an exception to a requirement or guideline of this policy should be addressed to the Associate Vice President of Technology Services.

TECHNOLOGY SERVICES RESPONSIBILITIES

5.01 Network Maintenance

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

5.02 Network Documentation

TS 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

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

5.04 Administration of University Network Name and Address Space

TS 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

TS coordinates use of wireless networking at the university to ensure compatible access to all university users.

5.06 Central Network Services

TS provides central services required for operation of the network.

5.07 Network Devices

The network is a mission critical strategic university resource. In order to protect the data communications network, devices other than end user devices such as computer, laptop, or mobile device must not connect to the network without written authorization from TS. This includes, but is not limited to, hubs, switches, repeaters, routers, servers, 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 confidentiality, integrity, and availability of the network.

5.08 Traffic Monitoring

TS monitors traffic flow to optimize network usage, predict future needs, detect network problems, ensure equitable access and for other properly authorized investigations.

5.09 Security Monitoring

To the extent possible, TS monitors incoming network traffic to detect the signatures of known network intrusion scenarios, viruses, or the like. TS may periodically scan the university network hosts to assess the vulnerability to attack. It should be noted that it is impossible to predict, detect, or prevent all potential system vulnerabilities.

5.10 Campus-Wide Network Security Coordination

TS promotes campus-wide network security and coordinates campus-wide response to unauthorized access. This 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

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

5.12 Upgrades to Current Infrastructure

TS performs upgrades to the current infrastructure to ensure current and future needs are addressed in conjunction with the OSUIT Strategic Plan and the OSUIT Technology Plan.

5.13 Upon being notified by unit leader and/or Human Resources of separation from the university, TS will immediately block all employee services using the OSU System

identity management system. Through integration with Active Directory this will block access to computers, network, and all other services.

USER RESPONSIBILITIES

6.01 The owners or primary users of computers connected to the university network are responsible for the following:

A. Abiding by all of OSUIT's IT Policies

Users should efficiently use network resources and follow OSUIT's official policies. Users are personally responsible for all activities logged to their user id and may be subject to disciplinary action and/or loss of privileges for misuse of computers or computing systems under their control.

B. Reporting Problems

Users should promptly report network problems to the TS service desk and cooperate with service support technicians in correcting malfunctions.

C. Taking Proper Security Precautions

Users should select secure passwords and change them regularly as described in OSUIT policy 6-004 *User Password Creation*. Security best practices must be used at all times.

D. Keeping the Operating System Secure

Users should make sure their computer's operating system is kept up-to-date with current security patches and must not open ports or disable firewalls.

6.02 Upon the separation of an employee by a unit leader and/or Human Resources, unit leader and/or Human Resources will immediately report the separation to Technology Services who will block all employee access using the OSU System identity management system. Through integration with Active Directory this will block access to computers, network, and all other services.

SPECIAL NOTIFICATIONS

7.01 OSUIT’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.

Approved: November 2004
Revised: July 2013
Revised: July 2016
Revised: December 2019