OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

850 - NETWORK INFRASTRUCTURE POLICY

SUBJECT: NETWORK INFRASTRUCTURE POLICY

NUMBER: 850

AUTHORIZING BODY: STRATEGY COUNCIL

RESPONSIBLE OFFICE: UNIVERSITY TECHNOLOGY SERVICES

DATE ISSUED: APRIL 2004

LAST UPDATE: FEBRUARY 2021

RATIONALE: This policy assigns responsibility for all aspects of creating, using, integrating, designing, installing, managing and maintaining Oakland University's (University) Network Infrastructure and its Core Network Services.

POLICY: This policy describes the guidelines for the use and expansion of the University wired and wireless campus network including integration with off-campus locations and cloud computing solutions. Use of the network, and growth and expansion of the network, must meet community expectations and provide consistent experience for the entire University community. University Technology Services (UTS) may prohibit or restrict network access for technical, regulatory compliance, legal, or policy considerations at any time.

SCOPE AND APPLICABILITY: The effective management of network information technology resources is important to the success of the teaching, learning and research mission of the University. Wired and Wireless Networks, including voice, data, and video networks, provide the communications backbone of the University. The challenge of networked environments is that more procedures and coordination are required as new information services are added (e.g. wireless communications).

DEFINITIONS:

Access Point: The electronic hardware that serves as a common connection point for devices in a Wireless Network. An Access Point acts as a network interface point

that is used to extend LAN segments, using Radio Frequency signals instead of electrical signals on a wire for access by multiple users of the Wireless Network. Access Points are shared bandwidth devices and can be connected to the Wired Network.

Core Network Services: Include, but are not limited to: Domain Name System (DNS); Dynamic Host Configuration Protocol (DHCP); Internet Protocol addressing (IP address); Media Access Control addressing (MAC); routing and switching; network connectivity; voice and data transmission; and Internet services.

Coverage: The geographical or building area where a baseline level of wireless connection service quality is provided or accessible, intentionally or unintentionally. In the case of a Wired Network, Coverage, for the purposes of this document, is defined as the local area network or network segment that is represented by the physical location of network drops or nodes on the network.

Domain Names: A name that identifies one or more IP addresses, Domain Names are used in Uniform Resource Locators (URL's) to identify particular web pages. UTS is responsible for maintenance of oakland.edu administration on the Educause web site registration service.

Firewall(s): A technical network implementation that protects computers on a specific network from intentional, accidental, hostile or unauthorized intrusion. Several firewall implementations may exist at any time, collectively referred to as Firewalls.

Guest Network: A wired or wireless network for use by OU guests, which may or may not require authentication. Service on a guest network is not guaranteed and can be revoked at any time.

Intrusion Detection Systems / Intrusion Prevention Systems (IDS/IPS): Devices, software applications, or combination device/software solutions that monitor network or system activities for malicious actions, attempted perimeter violations, or policy violations, and may log, report, issue alarms, or take automated actions.

Network Components: The individual devices such as drops, ports, hubs, routers and switches that support the technical implementation, connectivity, and the operation of the network.

Network Infrastructure: The inter-building and intra-building voice, data and video wired or wireless transport systems, and the electronic components and communication Protocols used to transport signals over the systems. In its simplest form, a network connects two or more computers together.

Network Resources: Systems, virtual servers, computational clusters, storage, printing and other items attached to the network that can be utilized through connection to the network.

Protocols: The defined format for communications transmission among devices, including the rules or sets of rules that create a communications and error handling standard.

Wired Network: Commonly referred to as "the network", Wired Network is the cabling infrastructure supporting all voice, video and data transmissions, as well as the routers, switches, and electronic components that facilitate technical communications. This may also be referred to as the "campus backbone network". The Wired Network begins at the point a device connects (i.e., a physical network drop or connection), continues through the campus in an intra-building mesh, and connects at a gateway to the Internet. The local access media may be fiber or copper, as appropriate for the technology.

Wireless Network: A local area network technology that uses radio frequency spectrum to connect electronic devices to the Wired Network. This may also be referred to as the wireless infrastructure, including Access Points, antennas, cabling, power and network devices used in the deployment of a Wireless Network.

PROCEDURES:

1. Network Management

    a. Responsibility

    UTS – Network Communications is responsible for the standards, design, implementation, performance and operation of the University Network Infrastructure, Core Network Services, Firewalls, IDS/IPS, Network Components, Protocols, Wired Network, and Wireless Network.

    UTS is responsible for monitoring compliance with this policy, within the scope of the Policy for Use of University Information Technology Resources.

    The Academic Computing Committee of the University Senate, and the Chief of Staff, will provide input and direction to UTS on network standards, design, implementation, performance and operation, of the University Network Infrastructure. UTS will work closely with Capital Planning and Design for network implementations in new and renovated facilities.

b. Delegation of responsibility

UTS may delegate operational aspects of Network Infrastructure support to academic or administrative units where a defined Service Level Agreement can be developed. In particular, UTS seeks to work with and support faculty members who are developing lab networks for educational and research purposes. UTS may also delegate responsibility to third party vendors when in the best interest of the University or the department. All delegations must be approved through consultation with UTS, Purchasing, Risk Management and Human Resources where appropriate.

2. Network Identity

a. Domain Name

Domain Names are essential to successful network addressing. Suggested Domain Names to be part of the Oakland University Network Infrastructure (cloud computing included) must be registered and approved by Communications and Marketing. Those establishing Domain Names must immediately notify UTS – Network Communications. Domains affiliated with the university network should end with "oakland.edu" when possible. University Communications and Marketing, at their sole discretion, maintains authority to prevent use of or revoke a domain name.

b. Global naming and addressing

UTS – Network Communications is responsible for providing a consistent forum for the identification and allocation of Internet Protocol (IP) addressing and naming conventions. Dynamic Host Configuration Protocol (DHCP) is the preferred method for the assignment of IP addresses. Exceptions to DHCP address assignment must be requested from UTS.

3. Access Guidelines

a. Access

Access to the Network Infrastructure will be provided to Oakland University faculty, staff, students, affiliates and guests, in a classification labeled "network users."

b. Authentication

Network users will be asked to register their network attached hardware and/or authenticate when connecting to the Oakland University network by using a University provided login identifier (NetID) and password. Wireless Network interfaces and computing devices will require user authentication to access the Wireless Network. Implementing network access with the

intent to bypass authentication will be considered a violation of this policy and a violation of the Policy for Use of University Information Technology Resources, unless the President, or his/her designee, has approved special provisions.

c. Authorization

Network users will be authorized through their network access to utilize specific Network Resources based on need. Access to educational and research resources is supported with open authorized access. Access to administrative and business operations requires specific “need to know” attached to job requirements, and requires approval by a supervisor. Network authorization will not define or create access where no need exists. Network authorization tools and strategies will implement and support the rules, guidelines, and strategies defined by the Policy for Use of University Information Technology Resources and Network Resource owners.

d. Devices connecting to the network

Functionality of any device is the responsibility of the owner. Any device (wired or wireless) connected to the network is subject to all university policies, particularly the Policy for Use of University Information Technology Resources, regardless of ownership.

e. NetID and Password maintenance

Network users will be prompted to change passwords on a periodic basis. Also, network users are to use the network login id NetID and passwords in a manner consistent with the OU AP&P #890 Use of University Information Technology Resources, and to protect and not share individual NetIDs and passwords with others.

f. Third Party/Backdoor Attachments

Attachments to the network by non-university organizations or network users must be approved by UTS, aligned with the OU AP&P #890 Use of University Information Technology Resources, and compliant with the Merit Network (www.merit.edu) third party connection and attachments policies.

4. General Usage and Connectivity Guidelines

a. Network Usage and connectivity

Use of the Network Infrastructure must be in a manner consistent with OU AP&P #890 Use of University Information Technology Resources. Equipment or network activity that violates this Network Policy will be subject to the disciplinary actions as outlined in OU AP&P #890 Use of University Information Technology Resources, which may include disconnecting or blocking such equipment or network activity.

b. Addressing

MAC and IP Addresses must be standardized in use and not altered or fraudulently presented. Alteration of addressing information is a violation of this policy and subject to sanction.

c. Planning

UTS must be involved in initial and ongoing planning and budgeting for all aspects of the Oakland University Network Infrastructure in existing structures, renovations, new structures, and remodeled areas, including planning for connectivity of the Oakland University Network Infrastructure to remote locations. UTS will seek to work with Capital Planning and Design, the University Senate Academic Computing Committee, and key representatives of units and departments in the Coverage area to ensure that Network Resource standards, requirements, interference minimization, and security are considered in the network plan.

d. Contracted network support

UTS will seek to work with Capital Planning and Design and key representatives of units and departments in the Coverage area to identify qualified contracted network support vendors meeting technical and security requirements. UTS – Network Communications must pre-approve all contracted vendor work on the University Network Infrastructure. All contracted vendor support work will be monitored for compliance to current University technical standards, quality installation and work completion in a timely manner. UTS may also choose to centrally sub-contract some operational and engineering network functions. Departments or Divisions will be assessed for the work and project management cost of tasks that require contracted network support.

e. Installation and removal of Network Components and Access Points

UTS – Network Communications must authorize the installation or removal of Network Components and Access Points prior to any work. Tampering with, altering, or moving Network Components or Access Points is prohibited unless prior approval is obtained through UTS. The location of all wireless Access Points must be coordinated with existing UTS plans.

f. Remote access services

Acceptable remote access to the Network Infrastructure, such as virtual private network, will be defined and maintained by UTS. UTS will seek to provide the most secure remote access connection appropriate to the security requirements defined by the affected Network Resource owners and managers. All external connections to the university network must first be reviewed and approved by UTS.

5. Additional Wireless Guidelines

a. Wireless Network legal restrictions

The special nature of Wireless Networks may be subject to legal restriction. Wireless Access Points must abide by all federal, state and local laws pertaining to Wireless Networks. UTS, working with the Office of Legal Affairs and the Office of Risk Management, is responsible for review of current technologies and legal restrictions. UTS will authorize the installation or design of wireless access with full consideration to this limitation.

b. Radio frequency spectrum

Prior to the implementation of a wireless technology, the unit acquiring and planning for the use of that technology must register and review the radio frequency spectrum with UTS.

c. Interference resolution

Certain wireless devices exist that utilize the same wireless frequency as the data network. In the event that a wireless device interferes with other equipment, UTS shall work with key representatives of units and departments in the Coverage area to seek resolution.

d. Wireless Network cards

Wireless Network cards are to be configured in client only mode and are not to be used as bridges, base stations, Access Points, or as an ad hoc network.

6. Regulatory Compliance, Security, and Firewalls

a. Security

UTS may take steps to preserve the security of the network and the security of devices connected to the network in line with the Policy for Use of University Information Technology Resources.

b. Protocols

UTS may take steps to preserve both security and quality of service by blocking or limiting Protocols identified as problematic.

c. Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems

UTS – Information Security Office is responsible for installing network security protections, such as Firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, or other network security systems to protect university assets. Firewalls are required at all Internet connections. Specific servers critical to University business and operations may be

protected behind such Firewalls, and those servers may be accessed for specific purposes as defined by the server or data owner.

Review of an existing Firewall, or a request for a new Firewall, may be initiated by contacting the UTS – Information Security Office. If a change in a network Firewall or other security device is needed, a Firewall change request form and ticket outlining the request must be submitted to UTS. These forms are available at forms.oakland.edu.

d. Security Reviews

UTS periodically performs security reviews such as vulnerability scanning and penetration testing, of any Network Resource, device, system, or component connected to the University network. Such reviews are done for the purpose of maintaining network and information security, at the request of a Network Resource, device, system or component client user, at the request of an authorized university representative, or in response to a legal or regulatory matter.

e. Compliance

Access Points, Core Network Services, Firewalls, IDS/IPS, Network Components, Network Infrastructure, Protocols, Wired Network and Wireless Network installations and implementations will be monitored by UTS – Network Communications and Information Security Office for conformance to established University plans, as well as regulatory compliance and industry best practices.

When Confidential Data (defined in OU AP&P #860 Information Security) are transmitted over the network, UTS – Information Security Office and Network Communications will enable and enforce measures to achieve regulatory compliance.

For specialized environments such as Payment Card Industry (PCI) and the Health Information Portability and Accountability Act (HIPAA), UTS – Network Communications will maintain a separate virtual local area network (VLAN). The VLAN will provide secure and encrypted data transmissions. Any component connecting to that VLAN will be managed through the standard UTS Change Management process.

UTS – Information Security Office and Network Communications will work with respective system administrator to maintain a network diagram that clearly indicates in-scope systems, segmentation, and support systems such as domain controllers, Intrusion Detection/Prevention System and sensors, and log aggregation tools. UTS – Information Security Office and Network Communications will maintain documentation for allowed ports and services.

UTS – Information Security Office and Network Communications will review Firewall and router rule sets every 6 months (January and July), review with the Security Advisory Committee, and submit an overview to the UTS Change Management Committee.

7. Peripheral and Auxiliary Networks

    a. Campus cable TV, fire alarm systems, automation or control systems, alarm systems, AV systems, surveillance cameras, or any other networked electronic or computer system that utilize the campus backbone or building wiring or co-locate with campus network facilities or electronics must be developed, installed, and operated in cooperation and coordination with UTS oversight. The system administrator or owner will maintain practices regarding the operation of each specific system (note OU AP&P #880 System Administration Responsibilities).

RELATED POLICIES AND FORMS:

OU AP&P #880 System Administration

OU AP&P #890 Use of University Information Technology Resources

APPENDIX: