



# University Network Administration

---

## 1. Policy Statement

- 1.1. The security, integrity, and availability of the Oregon State University (“university”) network is critical to the continued operation of the university. This policy regulates the use of the wired and Wi-Fi networks and the devices or systems used to access the University Network.

## 2. Reason for Policy

- 2.1. The University Network is a private network that exists to support the administrative, academic, research, and outreach activities of the university. This policy supports network availability and the appropriate physical and technical safeguards that provide optimum and secure performance without creating unjustified obstacles to the conduct of the business, teaching, outreach and research mission of the university and the provision of services to its many constituencies.

## 3. Scope & Audience

- 3.1. This policy applies to all university units, employees, students, agents, contractors, licensees, volunteers, and anyone who accesses the University Network.
- 3.2. Any system connected to the University Network, including subnetworks operated by individual units, is subject to this policy.

## 4. Definitions

- 4.1. **Cable Plant:** Fiber optic and copper cabling at all university locations delivering telephony, life safety systems, data networking, and wireless/cellular phone connectivity supplied by University Information Technology (UIT). Cable Plant includes all inter- and intrabuilding connectivity, pathways, communication rooms, spaces, and underground facilities such as maintenance vaults and conduits.
- 4.2. **Standards of Care:** For purposes of this policy, Standards of Care define minimum requirements for any device connected to or using the University Network.

- 4.3. **Internet:** An electronic communications network that connects computer networks and organizational computer facilities around the world.
- 4.4. **Local Area Network:** A local area network (LAN) is a computer network that links devices within a building or group of adjacent buildings.
- 4.5. **Network Administrator:** An employee within UIT, or a delegate appointed or designated by UIT, with authority to install and configure hardware and software for the University Network.
- 4.6. **University User:** An employee, student or other person with a current University Network systems account in good standing.
- 4.7. **University Network:** The infrastructure and equipment that connects computing devices to enable the exchange of data and information within the university campuses, research and instructional locations, and extension offices, and by connecting to the Internet, with the world. The University Network includes both physically wired and wireless (Wi-Fi) networks and the Cable Plant
- 4.8. **Wi-Fi:** A wireless LAN that uses radio waves to connect devices to the University Network and the Internet.

## 5. Responsibilities & Procedures

### 5.1. General

- 5.1.1. UIT is responsible for the University Network, including the Cable Plant, the physical and logical configuration of the University Network, and the university's connection to the Internet. Procurement and provision of University Network services to all university owned or controlled properties including, but not limited to, campuses, outlying locations, extension offices and research stations, is conducted and managed through UIT.
  - a. Any exception to Section 5.1.1 requires the prior written approval of the UIT Executive Director of Technical and Solutions Architecture or the Vice Provost for Information Technology & CIO.
- 5.1.2. UIT is responsible for procurement and provision of mobile wireless network services including but not limited to cellular and satellite-based services.
  - a. Any exception to Section 5.1.2 requires the prior written approval of the UIT Executive Director of Technical and Solutions Architecture or the Vice Provost for Information Technology & CIO.
- 5.1.3. UIT will:

- a. Authorize University Network system accounts and determine whether the accounts are in good standing;
- b. Monitor the performance and security of the entire University Network;
- c. Appoint and maintain a list of Network Operations Center (NOC) network administrators; and,
- d. Maintain a record of all devices registered to use the University Network.

## 5.2. **Wired University Network Resources**

- 5.2.1. All systems physically connected to the wired University Network must meet minimum automated authorization requirements regarding minimum configuration and security Standards of Care to provide for the protection and availability of the University Network.
- 5.2.2. All devices physically connected to the University Network must be named according to device naming conventions and logged in with a university user account to receive an IP address through the university's central IP address management system administered by UIT. This may be accomplished by direct registration with UIT or by automated data feeds from a college or division database.
- 5.2.3. All wired University Network hardware and software must meet defined Standards of Care to provide for the reliability and security of the University Network, and of the devices and data contained within the University Network. All installation, configuration and maintenance of University Network hardware and software must be conducted by or with approval of a UIT Network Administrator or a UIT-approved Network Administrator.
- 5.2.4. UIT Network Administrators and the Office of Information Security must have visibility and access into and may monitor all hardware and software on the University Network for security purposes.

## 5.3. **Wi-Fi (Wireless) University Network Resources**

- 5.3.1. No Wi-Fi infrastructure is permitted to connect to the University Network unless it is approved and installed by the UIT Network Operations Center. Installing unauthorized Wi-Fi access points is prohibited to avoid possible interference with the university Wi-Fi network, unnecessary impact to the wired University Network, and to minimize security risks to the university.
- 5.3.2. UIT may at its sole discretion add security services or capabilities to the wireless University Network to proactively enhance security remediation.

## 5.4. **Devices and Systems Connected to the University Network**

- 5.4.1. Only devices authenticated via an official university account, registered by a University User, or provided through an approved exception will be allowed to connect to the University Network.
  - a. Access to the *eduroam* Wi-Fi segment using *InCommon Federation* for authentication is an official university account for the purposes of this policy.
- 5.4.2. UIT will regularly monitor University Network activity and will notify users of any interfering devices that have the potential to impact the University Network. Devices found to be disruptive or an information security risk to the University Network in all university owned or controlled properties are prohibited and will be disconnected from the University Network.
- 5.4.3. The university, through UIT, reserves the right to disable network access to a device or an individual in the event of a misconfigured or compromised or malicious device, activities threatening the university's ability to continue to perform the operations of the university or resulting in a degradation of service, or a violation of a University Policy or Standard, university contract, or applicable law or regulation.
  - a. University Users believing their device or system has been wrongly disconnected or disabled from accessing the University Network may contact the UIT Service Desk for assistance.

## 5.5. Exceptions

- 5.5.1. The Vice Provost for Information Technology & CIO may grant exceptions to the requirements of this policy through procedures established by UIT.

## 6. Related Policies, Procedures, or Information

- 6.1. *Standards of Care* are described and documented on the UIT website, available at <https://uit.oregonstate.edu/infosec/infosec-guidebook/baseline-standards-care>.

## History

Oregon State University adopted University Policy 08-010 *University Network Administration* on September 14, 2016. University Policy 08-010 *University Network Administration* was reviewed and received housekeeping amendments pursuant to its periodic review on August 6, 2024.

Next scheduled review date: August 2029.

## Contacts

### **UIT Service Desk**

541-737-8787

<https://uit.oregonstate.edu/help-support>

### **UIT Network & Telecom Services**

541-713-HELP

<http://uit.oregonstate.edu>

Available online at: [https://policy.oregonstate.edu/UPSM/08-010\\_university\\_network\\_administration](https://policy.oregonstate.edu/UPSM/08-010_university_network_administration)