BOISE STATE UNIVERSITY

University Policy 8010

Network Standards

Effective Date

November 1997

Last Revision Date

April 07, 2022

Responsible Party

Office of Information Technology, (208) 426-4357

Scope and Audience

This policy applies to all members of the University community and users of the University Network.

Additional Authority

- Communications Act of 1934 (amended)
- The Family Educational Rights and Privacy Act of 1974 (FERPA)
- The Computer Fraud and Abuse Act of 1986
- The Computer Virus Eradication Act of 1989
- The Electronic Communications Privacy Act
- Idaho Code Title 18, Chapter 22 (The Idaho Computer Crimes Statute)
- Idaho Technology Authority policies
- University Policy 2020 (The Student Code of Conduct)
- University Policy 8000 (Information Technology Resource Use)
- University Policy 8020 (Server Administration)
- University Policy 12020 (Exclusion from Campus)

1. Policy Purpose

To clarify standards to protect the data and Network-related resources of the university by providing secure and consistent Network access, maintenance, and methodologies.

2. Policy Statement

Boise State University supports centralized Network services to offer the most advanced technology available while ensuring that stable and reliable services are maintained for the benefit of the University community.

3. Definitions

3.1 Network Engineer

The senior certified technical employee in the Office of Information Technology who is responsible for the University Network. The Network Engineer may either be a position title or a specific position designated by the Chief Information Officer for OIT.

3.2 Telecommunications Rooms

Equipment rooms that house Network cabling, cross-connect panels, and Network electronics. Each building has one entrance facility serving as a point where inter-building entrance cables (fiber) terminate called an entrance facility, or a building distribution frame room and one (1) or more satellite Telecommunication Rooms to redistribute connections called intermediate distribution frame (IDF) rooms.

3.3 University Network/Network

All cabling (copper and fiber) as well as point-to-point wireless, connected buildings and equipment within buildings ending at the data faceplate into which a user plugs a patch cable from their device, etc. The University Network also includes all switches, wireless access points, and routers providing connectivity. In addition, the Network includes all Wide Area Network (WAN) equipment, firewalls, and Network scanners.

4. Office of Information Technology (OIT) Responsibilities

4.1 Network

OIT is solely responsible for the entire University Network. Specifically, OIT is responsible for:

a. Administering all data lines (fiber and copper) installed on University property.

b. Installing or contracting to install data lines (fiber and copper).

c. Supporting the university's basic communications/Network.

d. Managing the use of all data lines and projecting future needs.

e. Installing and/or managing switches and wireless access points on the Network.

f. Operating routers on the Network and installing or configuring any device to route on the Network.

g. Maintaining all enterprise Networking equipment purchased with University funds and installed in the Network. OIT may grant exceptions to: 1) assist campus departments and units that have purchased equipment outside of OIT funding, or 2) grant on-going maintenance access to faculty or staff with specialized equipment.

h. Maintaining all WAN data connections to the university.

i. Extending the Network. All requests to extend the Network (e.g., IP tunneling, WAN connections, WAN upgrades, etc.) must be forwarded to the University Network Engineer.

4.2 Telecommunications Rooms

a. OIT exclusively manages University Telecommunications Rooms.

b. Access to Telecommunications Rooms for non-OIT staff must be coordinated through OIT Telephone/Network Services.

c. Access card entry is required on all telecommunications doors for access control, auditing, and security purposes.

d. Telecommunication rooms must be dedicated spaces that are not accessed by other departments or units or used for storage or janitorial purposes. Telecommunication rooms must be outfitted with appropriate cooling and ventilation for Networking equipment. Rooms must be outfitted with electronic door access that maintains an access log.

e. Telecommunication rooms that serve as Network cores for multiple campus buildings must be equipped to data center standards TIA 942 to include adequate power, cooling, uninterruptible power sources, and chemical fire suppression.

4.3 Separate Networks

a. OIT must authorize the design and implementation of any college, school, or department's separate Network.

b. OIT is responsible for the protection of the University Network. Initial and ongoing costs of a separate Network will be the responsibility of the requesting academic or auxiliary unit.

c. OIT will work with campus leadership to educate faculty, students, and staff on the shared responsibility of Network access, as needed.

4.4 Network Addressing

The Network Engineer will manage the process and methodology of addressing for all equipment that uses the Network. The improper use of Network addressing is a violation of this policy.

4.5 Wireless Guidelines

a. The University provides wireless access to computing and IT resources for employees, affiliates, students, vendors, and guests as part of the services offered to enhance productivity. Wireless Networks operate within a shared and finite radio spectrum. OIT will maintain administrative rights over this spectrum on campus and remote University buildings to ensure the fair and efficient allocation of resources.

b. OIT will manage the RF (radio frequency) spectrum and reserve specific 20mhz wide 5ghz channels for use by non-OIT departments and vendors. Departments and vendors may only use the assigned channels.

c. OIT will grant, limit, or restrict access to the wireless spectrum within the physical spaces and on grounds owned or controlled by the university.

d. OIT will monitor the spectrum on a continuous basis and may regulate all wireless activities at all University sites, including remote offices and common areas.

e. OIT, or designee, may cause or request immediate deactivation of any device creating harmful interference until such device can be reactivated without causing harmful interference.

4.6 Acceptable Usage

Access to Networks owned or operated by the university imposes certain responsibilities and obligations and is granted subject to University policies and federal, state, and local laws. Acceptable use of Networks includes but is not limited to the following:

a. Respecting system security mechanisms and not taking measures designed to circumvent, ignore, or break such mechanisms,

b. Showing consideration for the consumption and utilization of IT resources, such as ensuring that a user or process has not exceeded established limits placed on the services, or ensuring that a user does not consume a resource to a level such that the service to other users is degraded or where the actions of the user could cause degradation if the user was permitted to continue the practice or activity (see University Policy 8000 - Information Technology Resource Use), and

c. Assisting in the performance of remediation steps in the event of a detected vulnerability or compromise.

4.7 Limited Privacy Expectations

While the University respects a user's privacy, the University cannot ensure any level of privacy (see University Policy 8000 - Information Technology Resource Use).

4.8 Monitoring and Enforcement

a. Information technology resources must be available to support the University's mission. The university reserves the right to inspect such resources to maintain or improve functionality, or if there is a suspicion of misconduct or a potential violation of federal, state, local law, or University policy.

b. Offenders may be prosecuted under all applicable laws, including but not limited to, the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, the Idaho Computer Crimes Statute, and the Electronic Communications Privacy Act.

4.9 Disclaimer

a. An individual using a Network owned by the university does so subject to applicable laws and University policies. A user assumes all associated risks and agrees to hold Boise State University and its employees harmless for: 1) the compromise of any personal information (e.g., credit card numbers); 2) any damage caused to users' hardware or software due to security issues; or 3) any other harm caused by viruses or hacking while on University Networks.

b. Boise State University disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible Networks.

c. Materials on university and non-university systems do not necessarily reflect the attitudes, opinions, or values of the university, its faculty, staff, or students.

4.10 Problem Resolution

The responsibility of connectivity to the Network and the services it provides is shared equally by all members of the University community. In the event of an incident that affects the ability of end-users to access the Network, OIT will take all appropriate steps necessary to fix the problem. In the event that an incident occurs off-hours, the senior person in Technology Services will follow the Emergency Response Plan which may result in the disconnection of a building or the rerouting of fiber.

5. Policy Non-Compliance

a. Suspected violations of this policy should be reported to the appropriate supervisor, department head, Dean, Vice President, or to OIT.

b. Reported violations will be evaluated on a case-by-case basis and may result in:

- Referral to the Office of the Dean of Students for student violations, which may result in action through the Student Code of Conduct (University Policy 2020).
- Referral to Human Resources for employee violations, which may result in discipline, up to and including dismissal.
- Exclusion from campus under University Policy 12020 (Exclusion from Campus).

- Civil and/or criminal liability.

6. Related Information

Emergency Response Plan
https://www.boisestate.edu/oit/itgrc/it-plans-procedures/cyber-incident-response-plan/

Last Review Date

July 12, 2024

Revision History

March 2015; April 07, 2022