BOISE STATE UNIVERSITY

University Policy 8010

Network Standards

Effective Date

November 1997

Last Revision Date

March 2015

Responsible Party

Vice President and Chief Financial Officer, (208) 426-1200
Chief Information Officer, (208) 426-5774

Scope and Audience

This policy applies to all members of the Boise State University community, and users of the University Data Backbone.

Additional Authority

- 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
- Idaho Code Title 18, Chapter 22 (The Idaho Computer Crimes Statute)
- The Electronic Communications Privacy Act
- University Policy 2020 (The Student Code of Conduct)
- University Policy 8000 (Information Technology Use)
- University Policy 8020 (Server Administration)
- University Policy 12020 (Exclusion from Campus).

1. Policy Purpose

This policy protects the data and network-related resources of the University. It helps ensure a secure and reliable network available twenty-four hours a day, seven days a week in which end-users have confidence. It reduces the risk of data loss or loss of service by providing 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 Data Backbone, Backbone

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

3.2 Network Engineer

The senior certified technical employee in OIT that is responsible for the University data network. This position is either an employee title or a position that is identified by the CIO, OIT.

3.3 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 or more satellite Telecommunication Rooms to re-distribute connections called intermediate distribution frame rooms.

4. OIT Responsibilities

4.1. Backbone

OIT is solely responsible for the entire Boise State University Data Backbone. Specifically, OIT is responsible for:

a. Administering all data lines (fiber and copper) installed at Boise State University, including those not on the main campus.

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

c. Providing, funding, and supporting the University's basic communications/Data Backbone. Managing the use of all data lines and project future needs.

d. Install and/or manage switches, and wireless access points on the Data Backbone.

e. Operating routers on the Data Backbone, and installing or configuring any device to route on the Backbone.

f. Maintaining all Data Backbone networking equipment purchased with University funds and installed in the Backbone. OIT may grant exceptions to a) assist campus units that have purchased equipment outside of OIT funding, or b) grant on-going maintenance access to faculty or staff with specialized equipment.

g. Maintaining all WAN data connections to the University.

h. Extending the Data Backbone. All requests to extend the Data Backbone (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 with OIT Telephone/Network Services.

4.3 Separate Networks

a. OIT must set up and maintain any college or department's separate networks.

b. OIT is responsible for the protection of the University network, but initial and ongoing costs of a separate network will be the responsibility of the requesting academic or auxiliary unit.

4.4 Services

4.4.1 IP Addresses

The Class B IP address block 132.178.0.0/16 and BSU-IPV6 block 2620:109:5000::/44 are the property of Boise State University. The Network Engineer will manage the addresses (numbers) and their use. The improper use of University IP numbers is a violation this policy.

4.4.2 Dynamic Host Configuration Protocol (DHCP)

a. DHCP is a protocol that provides a means to dynamically allocate IP addresses.

b. OIT is responsible for DHCP implementation and service.

4.4.3 Domain Name System (DNS)

a. DNS is a general-purpose distributed and replicated data query service chiefly used on the Internet for translating hostnames into Internet addresses, as well as the style of hostname used on the Internet (though such a name is properly called a fully-qualified domain name).

b. OIT is responsible for DNS service on the Network.

4.4.4 Protocols

The only authorized routed protocol on the Boise State University network is Transmission Control Protocol/Internet Protocol (TCP/IP).

4.5 Wireless Guidelines

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

4.5.1 Access

a. The University provides wireless access to computing and IT resources for employees, associates, students, and guests as part of the services offered to enhance productivity in the workplace. 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 fair and efficient allocation of resources.

b. OIT will manage the RF spectrum and reserve specific 20mhz wide 5ghz channels for use by non OIT departments and vendors. Departments and vendors shall only use the assigned channels.

c. The spectrum usage applies to all device traffic and interference occurring in the following frequencies ranges:

- 800 and 900 MHz, industrial, scientific, and medical (IS) bands, all modes
- 2.21920-1930 MHz, all modes
- 2.4-5 GHz, all modes
- 4.9-6 GHz, all modes

4.5.2 Wireless Spectrum

a. OIT will grant, limit, or restrict access to the wireless spectrum within the physical spaces and on grounds owned and operated by Boise State University.

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

c. Should any device create harmful interference, OIT or their designee may request immediate or cause deactivation of the device until such time as it can be reactivated without causing harmful interference.

4.5.3 Acceptable Usage

Access to wireless networks owned or operated by Boise State imposes certain responsibilities and obligations and is granted subject to University polices, and local, state, and federal laws. Acceptable use of wireless networks includes, but is not limited to the following:

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

b. Showing consideration for the consumption and utilization of IT resources, and

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

4.5.4 Privacy Expectations

While the University respects users' rights to privacy, the institution cannot assure any level of privacy as stated in University Policy 8000 (Information Technology Use). Users are responsible for taking reasonable measures to ensure their own privacy on the wireless network.

4.5.5 Wireless Monitoring and Enforcement

a. Information technology resources must be available to support the University's mission. Staff may need to inspect the resources to maintain or improve the function, if there is a suspicion of misconduct or if there may be a violation of Federal, State, local law or evidence of violation of 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.

4.5.6 Wireless Disclaimer

a. Individuals using wireless networks owned by Boise State do so subject to applicable laws and Boise State policies. Users assume all associated risks and agree to hold Boise State 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 Boise State wireless networks.

b. Boise State disclaims any responsibility and/or warranties for information and materials residing on non-University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions, or values of Boise State, its faculty, staff, or students.

4.6 Problem Resolution

The responsibility of connectivity to the Data Network and the services it provides is shared equally by all Boise State University members. In the event of an incident that affects the ability of end-users to access the Data Backbone, OIT will take whatever 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 re-routing of fiber.

5. Policy Non-Compliance

Violation of any portion of this policy may result in disciplinary action. Incidents will be evaluated on a case by case basis and may result in the following sanctions up to:

a. Exclusion or expulsion, in the case of students as outlined in the Student Code of Conduct, or

b. Exclusion or dismissal from employment, in the case of faculty and staff, or

c. Exclusion from campus, in the case of the public.

Revision History

March 2015