

---

## NETWORK STANDARDS

---

**PURPOSE:** This policy was created to protect the data and network-related resources of the University, to provide a secure and reliable network available twenty-four hours a day, seven days a week in which end-users have confidence, and to reduce the risk of data loss or loss of service by ensuring consistent network access, maintenance, and methodologies.

### I. Policy Statement

Boise State University supports decentralized network services. *The Office of Information Technology* (OIT) is ultimately responsible for the Boise State University *backbone*. Organizations choosing to install and manage edge equipment are responsible for funding and supporting edge equipment and connectivity.

A. Backbone: The Office of Information Technology (OIT) is solely responsible for the entire Boise State University backbone.

1. OIT is the sole administrator of all data lines (fiber and copper) installed at Boise State University.
2. Only OIT will install or contract to install data lines (fiber and copper).
3. OIT, rather than colleges or departments, has the responsibility to provide, fund, and support the University's basic communications backbone utility. Colleges, departments, and offices will pay for the installation of new data lines beyond those provided as part of the University's basic communications backbone utility and for the movement of existing data lines to end-users.
4. OIT will catalog and manage the use of all data lines and project future needs.
5. OIT will install and/or manage hubs, switches, and wireless access points on the backbone.
6. Qualified IT Staff may install and/or manage edge switches and wireless access points with the approval of the University Network Engineer.
7. Only the University Network Engineer will operate bridges on the backbone. No one except the University Network Engineer will install or configure any device to bridge protocols or networks on the backbone (e.g., Localtalk to Ethertalk bridge, any PC with 2 NIC cards).
8. Only the University Network Engineer will operate routers on the backbone. No one except the University Network Engineer will install or configure any device to route on the backbone (e.g., routing on NT workstations, WIN 95, Apple workstations, Apple servers, Novell servers, NT servers, Unix servers).
9. All backbone networking equipment purchased with Boise State University funds or acquired for use at Boise State University and installed in the backbone becomes the sole responsibility of OIT.

10. Qualified IT Staff may operate hardware based security devices, firewalls, or devices that filter or scan traffic on an as-needed basis on the University's backbone, with the approval of the University Network Engineer.
  11. The University's Network Engineer is responsible for all WAN data connections to the University.
  12. No organization except OIT will extend the University's backbone. All requests to extend the backbone (e.g., IP tunneling, WAN connections, WAN upgrades, etc.) will be forwarded to the University's Network Engineer.
  13. Organizations requesting new file servers will do so in accordance with Boise State University policy [BSU 8020](#).
- B. OIT Telecommunications Rooms (Telco's)
1. *Telco's* that have been built to support telecommunications exclusively or remodeled to remove janitorial, supply, electrical, or other non-telecommunication related services in order to support telecommunications exclusively are assigned to OIT by the University's Facilities Management Council.
  2. These *Telco's* shall be keyed to an OIT Master Key. All new construction and building remodeling will include provisions for meeting the telecommunications cabling and design guideline standards set by OIT.
  3. The Executive Director of OIT may grant access to qualified IT Staff members. For colleges, departments or offices with qualified IT Staff authorized to access OIT assigned *Telco's*, a single key per building will be issued to the dean or director. The key is to be located in a secure environment and a log-file kept regarding its use.
  4. Only the Executive Director of OIT shall approve access and keys.
  5. Colleges, departments or offices that are granted access to OIT assigned *Telco's* will assist in funding and maintaining those *Telco's*.
  6. Qualified IT Staff granted access to OIT *Telco's* are authorized:
    - a) access twenty-four hours per day, seven days per week,
    - b) the ability to physically review and identify connections and identify power and/or equipment problems,
    - c) the ability to connect with patch cords – workstations, servers, and printers to an edge switch that is managed by that IT Staff member's organization (Adding users to backbone switches or other organization-managed switches is not permitted.).
  7. IT Staff members shall:
    - a) provide advance written notice of the installation of any electronics in the *Telco's* to the other organization's point of contact. Exempted from this notification are UPS's. No servers or computers will be installed in any *Telco's* (except Hub Facilities). Any equipment that needs cross connection between equipment of different organizations will be coordinated in advance.
    - b) annotate and maintain activity logs in the *Telco's* on the log sheets provided.
    - c) adhere to wiring standards in the *Telco's* as set forth by Telephone Services and BSU Facilities Master Specifications.

### C. Separate Networks

The University Network Engineer will work with any college or department to assist in the setup and maintenance of a separate network for academic purposes.

1. If needed, the separate network may be attached to the backbone, if sufficient protection is implemented and maintained so as to prevent any detriment to the Boise State University network.
2. Separate academic networks are the sole responsibility of the associated academic unit.

### D. Services

#### 1. IP Addresses

- a) The Class B IP address license “132.178.0.0” is the property of Boise State University.
- b) The University Network Engineer will manage the addresses (numbers) and their use.

#### 2. Dial-Up

- a) No unauthenticated dial-ups are permitted to any device connected to the University network.
- b) All requests for analog lines for modem connections will be forwarded through the Manager of Telephone and Network Services along with a statement explaining the need for dial-up services and the measure(s) taken to control and/or prevent the user from accessing the network for misuse or unauthorized activities.

#### 3. Dynamic Host Configuration Protocol (DHCP)

- a) DHCP is a protocol that provides a means to dynamically allocate IP addresses.
- b) The University Network Engineer is responsible for DHCP implementation and service.

#### 4. 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) The University Network Engineer is responsible for DNS service on the Boise State University network.

#### 5. Protocols – The only authorized routed protocol on the Boise State University network is TCP/IP.

### E. Best Practices

Managers of Boise State University IT resources shall seek and adopt whenever possible *best practices* with regards to the acquisition, implementation, management, and replacement of IT resources. The Network Administrators Group shall review and adopt appropriate standards and procedures that represent *best practices*.

## II. Scope

This policy applies to all colleges, departments, and offices of Boise State University, including all devices attached to the Boise State University backbone, and is meant to enhance the academic and business functions of the University.

## III. Definitions

A. Backbone

The *backbone* includes: all cabling, both copper and fiber, as well as point-to-point wireless, connecting buildings, and equipment within buildings, ending at the data face plate into which a user plugs a patch cable from his/her computer, printer, etc. The Boise State University *backbone* also includes all hubs, switches, wireless access points, and routers providing connectivity. In addition, the backbone includes all Wide Area Network (WAN) equipment (e.g., CSU/DSUs), firewalls, and scanners.

B. Backbone Switches

*Backbone switches* are any switches that are not edge switches or server farm switches. Every building has a building switch for the *Private Segment* (and sometimes the *Public Segment*) that is located in the entrance facility. This is the distribution switch from the main campus backbone. Edge switches are attached to this distribution (*backbone*) switch. User connections are then attached to the edge switches. The server farm switch is connected to the distribution switch and has servers attached to it rather than users.

C. Best Practices

*Best practices* are those data management and network procedures generally recognized by the industry for assuring secure, reliable, scaleable, and efficient data repositories and networks.

D. Private Segment

The private segment includes machines that do not require initial access from the Internet. It also includes machines that can be associated with a specific user, a very small group of people, or machines that need the higher safety or security provided by the private segment of the Boise State University Network.

1. Private segment computers include, but are not limited to:

- a) Faculty, Staff, and Administrative network devices;
- b) Closed labs or labs that are primarily research labs;
- c) Computers containing sensitive information, such as student, health or financial information.

E. Public Segment

The *public segment* includes machines that require initial access from the Internet. Also, machines that cannot be associated with one person, a very small number of people, or that provide a higher security risk will be hosted on the public segment of the Boise State University Network.

1. These include the following, but are not limited to:

- a) Dial-in access to the LAN and remote access through remote control software;
- b) Web servers, etc.;
- c) Wireless access points;
- d) Open computer labs.

F. Qualified IT Staff

The *Qualified IT Staff* is composed of information technology employees of the University who are qualified or actively working on and demonstrating satisfactory progress towards qualification. Qualification shall be agreed upon on an individual basis between the Executive Director of IT and the employee's dean or director. *IT Staff* includes staff assigned to OIT, colleges or departments with titles including but

not limited to Systems Administrators, Systems Engineers, Network Engineers, or Telecommunications Technicians.

G. Telecommunications Rooms (Telco's)

Telco's are equipment rooms that house network cabling, cross-connect panels, and network electronics. Each building has one *Telco* serving as a point where inter-building entrance cables (fiber) terminate called an *entrance facility* or a *Building Distribution Frame* room (BDF), and one or more satellite Telco's to re-distribute connections called *Intermediate Distribution Frame* rooms (IDF's).

IV. Responsibility

Organizations that modify end-user connections to edge switches are then responsible for responding to end-user support requirements for network connectivity to those switches.

IT Staff are ultimately accountable to the respective dean or director. A distributed, collaborative environment is unique and any unforeseen issues or problems shall be handled through the proper reporting structure by the dean or director and the Executive Director for IT. Failure to adhere to these policies as determined by the Executive Director of IT in consultation with the IT Staff member's dean or director may result in the loss of access to Telco's by the offending IT Staff member.

A. Modification of Policy

1. The Executive Director of *Information Technology* (IT) is responsible for administering this policy, including its maintenance and compliance.
2. A subcommittee of the Network Administrators Group (the Network Policy Subcommittee) will review this Policy periodically and make recommendations regarding additions, deletions and/or modifications to the Executive Director of IT. Others wishing to make recommendations may make them directly to the Executive Director of IT.

B. Exceptions to Policy

1. Any college, department or office that wishes an exception to this policy must present its written request to the Network Policy Subcommittee.
2. The Network Policy Subcommittee will review and forward the request with the Subcommittee's recommendation to the Executive Director of IT. The Executive Director of IT will then either approve or deny the exception. The Subcommittee's recommendation and the decision from Executive Director of IT will be forwarded to the requesting party within thirty days.
3. Only the Executive Director of IT may authorize an exception to this policy.

V. Procedures

The Class B IP address license 132.178.0.0 is the property of BSU. The Network Engineer will manage the addresses (numbers) and their use. The improper use of BSU IP numbers is a violation of the BSU Computer Use Policy.

A. Emergency Response

The privilege of connectivity to the Boise State University 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 backbone, the University Network Engineer will take whatever steps necessary. This could mean disconnecting a building because of a faulty component or re-routing fiber connections. In the event that an incident occurs off-hours, the senior person in Computing Services will follow

the emergency response plan, which may result in the disconnection of a building or the re-routing of fiber.

B. Non-Compliance with this Policy

1. First offense – non-compliance with this policy will result in a warning notice being sent by the Network Administrators Group Chair to the responsible System Administrator by e-mail or letter. The warning notice shall include a description of the violation referencing the Network Policy and recommending the necessary corrective action and acceptable time frame for required actions to be completed.
2. Second offense – a second offence of non-compliance with this policy will result in a warning notice of non-compliance from the Network Administrators Group Chair to the responsible System Administrator with copies to the appropriate Dean or Director and the Executive Director of IT. The warning notice shall include a description of the violation referencing the Network Policy and requiring immediate corrective action.
3. Continued offenses – a third violation of this Policy will result in the termination of network services to the offending department or college. The Executive Director of IT will direct a notice to the appropriate Dean or Director with a copy to the IT Governance Council. Such services will not be re-established until the Network Subcommittee notifies the Executive Director of IT that the violation has been resolved in accordance with established policy.