

Network Use Policy

BYU-Idaho owns and operates a network to help fulfill the institution's mission. Only those who are authorized are allowed to use the network and they must abide by certain rules. The Information Technology (IT) department will manage the network in such a way as to insure confidentiality, integrity and availability of data.

The network has been provided as a critical tool to allow employees and students to conduct the business of education. All use of the network should be in conformance to the honor code and the objectives of The Church of Jesus Christ of Latter-day Saints. All use of the network is also governed by the policies and guidelines outlined in the Acceptable Use Policy. Network access and use must also abide by local, state and federal laws.

Those who are allowed to use the network are:

- Employees who have a need to be on the network to perform their work duties.
- Students who have network access through labs, public access ports, wireless access, or live in on-campus housing.
- Guests who receive temporary permission to access the network through public access port or wireless access.

Those who use the network shall:

- Login using their own NetId and password.
- Have up-to-date antivirus software.
- Use the network only for lawful and legitimate purposes intended by BYU-Idaho.

Network Security

All users are forbidden to alter physical network resources without proper authorization. Users shall not extend, modify, or tamper with existing network elements, including but not limited to switches, routers, gateways, wireless access points, wiring/cabling and University owned computers. Users shall not install servers without express permission from the BYU-Idaho IT Department and BYU-Idaho administration. Users shall not provide any network access or services to other computers. For example, under no circumstances shall users provide domain name services (DNS) or dynamic host control protocol (DHCP) as this can cause loss of network availability to all other users.

NetID and Password

All access to the BYU-Idaho network must be authorized through a valid NetID and password. The NetID and password are chosen by the student upon enrollment at the university or chosen by the employee/faculty upon hiring. Conventions and requirements for the NetID and password are covered in the Information Systems Security Policy.

Monitoring and Loss of Privileges

BYU-Idaho IT manages the network and is authorized to review and monitor the use of the system to determine compliance with policy and law. Upon discovery of inappropriate activity, IT may share such information with authorized persons for official

purposes, including law enforcement agencies. IT may revoke access to the network when deemed appropriate or necessary.

Firewall and Filtering

BYU-Idaho IT limits and filters access to particular systems for security, honor code, and service reasons. The confidentiality, integrity, and availability of network servers and data are insured by the use of firewalls, filtering, and etc. Access to sites or services that violate the intent of the honor code or copyright laws and sites or services that waste limited bandwidth are blocked according to conventions set by management. Users shall not tamper with or bypass the blocking software. Exceptions to firewall, filtering, and such management practices may be requested through the IT office.

Disk Space

All users of the BYU-Idaho network are allotted a specific amount of disk space according to their position (student, faculty, employee, etc.). All users are required to keep their disk space clear of unnecessary data and stay within the limits of the disk space allotted to them. In some cases, students working for the university can qualify for a larger disk space. Such cases should be referred to the Information Technology department.

Network Access Privileges

All authorized users are able to access the Internet through the on-campus network. Because of limited bandwidth for a large number of users, the network internet connection should not be used to download large files not related to University business from the internet, especially streaming video/audio.

All users may print documents using the Pharos printing network or applicable printer, depending on the department. Users must have the required amount of money in their accounts in order to use the Pharos system.

Users may access their email service through the Outlook server. Student email, as well as Blackboard and personal accounts, and registration information can also be accessed through the my.byui.edu portal on the BYU-Idaho website.

Wireless Access

Users may access the network wirelessly through the university Wi-Fi hotspots and must abide by the Wireless Policy. Computers accessing the network must be running anti-virus software with current updates. Computers with peer-to-peer file sharing software will either be denied access to the network or only allowed limited access.

Remote Access

The BYU-Idaho web site and portals and most required services may be accessed off-campus through an internet connection with a valid NetID and password. Employees who require special remote services from off campus may apply to the IT office for a virtual private network (VPN) account, which is subject to the Remote Access policy.

Housing

BYU-Idaho provides network access for students living in on-campus housing with compatible computers. The Help Desk will assist with the initial setup and ongoing support.

The student's PC network configuration will be changed, including its name to reflect its location and owner, making it easily identifiable. Students agree not to modify the network configuration, since it can cause network failure or problems.

The student is required to have up-to-date anti-virus software and operating system security patches. The student takes responsibility for maintenance and up-keep of his or her own PC and will not hold the University responsible for viruses contracted through the network.

Each network jack will be used only for one network connection. Students shall not attempt to connect multiple systems to one network jack, but they are allowed to switch back and forth where there is only one jack and two computers. Students will not host servers nor provide services on the network, for example audio servers, video servers, games, web business, etc. Students shall not provide any dial-up services to the network. They will not simultaneously use their modem and network connection; they will physically have one unplugged while using the other. Students will not use the network for any kind of business or commercial advertising.

Special Purpose Network

A special purpose network is built to fulfill a specific need. For example, a class that teaches networking or computer security has special needs that must be handled separate from the rest of the network. Such needs, when brought to the attention of IT and approved by administration, will be built according to mutually agreed upon terms between IT and the customer.

Lab Use

All computer labs are required to be locked when not being supervised by authorized faculty or lab assistants. Computer labs may only install new software at the beginning of each semester and should have all software approved through the IT department. (see Computer Lab Software Imaging Policy)

IT Tours

Tours of IT areas are discouraged for security reasons. Exceptions for reason of educational value can be requested at the office of IT. When approved, tours will be scheduled and groups must be kept small enough to be easily managed.

Enforcement

BYU-Idaho administration reserves the right to actively monitor network use and insure compliance to policies. Anyone found abusing the privilege may lose access to the network and face disciplinary action, including dismissal from school and legal action.