

Computer Security and Use Policy

BYU-Idaho owns, operates, and maintains computers and private networks for the purpose of meeting the objectives of its mission statement. Computer and network access for patrons, hereafter called users, is restricted to authorized faculty, staff, students, and others who have been approved by appropriate administrators. The networks and computing resources at BYU-Idaho provide students and employees with many capabilities. With these benefits come responsibilities and obligations required of those who use university provided resources. Users must use those resources in an ethical and legal manner, consistent with University policy, the BYU-Idaho Honor Code and applicable laws of the land.

Users shall:

- Use resources for authorized and lawful purposes only and follow authorized procedures in this use.
- Connect to the network, whether wired, wireless, local or remote, only through campus approved and provided means.
- Ensure network devices, whether university or privately owned, meet University established minimum standards of security including, but not limited to, up-to-date virus protection and operating system security patches.
- Access only information to which they have been authorized.
- Protect individual accounts and passwords and not share them with others.
- Abide by copyright law, respect the intellectual property of others, and abide by the provisions of applicable license agreements.

Users shall not:

- Use another person's user account or password.
- Use another person's computer system, software, files or data without appropriate authorization.
- Use computer programs to decode passwords, access control information, or intercept, decode, or disrupt transmissions.
- Attempt to circumvent or subvert system security measures or filtering systems by any means.
- Attempt unauthorized access of the campus networks or use devices that extend the network including, but not limited to, hubs and wireless access points.
- Knowingly engage in any activity that causes harm to computers or information stored thereon, such as creating or propagating viruses, damaging files, spamming, or any other use that degrades or disrupts services.
- Change existing network cabling or configuration.
- Use computers or wireless network devices for personal business or political purposes.
- Harass, stalk, post or transmit anything threatening, annoying, abusive, fraudulent, hateful, or obscene. (See E-mail policy)

BYU-Idaho considers any violation of this policy to be a serious breach of conditions for employment or academic standing. BYU-Idaho reserves the right to copy and/or examine any files or information that reside on the network or on BYU-Idaho property that is related to any use of its resources. Violators of this policy are subject to the full range of disciplinary actions as described in applicable BYU-Idaho Policy, including dismissal from employment or separation from the university, and may also be sued or prosecuted under applicable local, state, or federal civil and/or criminal law. Unacceptable computer use includes any computer activity that does not comply with this policy, the Honor Code, with the principles and standards of The Church of Jesus Christ of Latter-day Saints, or actions that would injure the reputation of BYU-Idaho, or any other misuse of campus computing resources which, in the sole discretion of the University, would be injurious to BYU-Idaho.

Any exceptions to this policy must receive written authorization from the Computer and Technology Council (CTC).