BOISE STATE UNIVERSITY

University Policy 8000

Information Technology Resource Use

Effective Date

November 1997

Last Revision Date

February 07, 2022

Responsible Party

Office of Information Technology, (208) 426-4357

Scope and Audience

This policy applies to all users of University Information Technology (IT) Resources.

Additional Authority

- Family Educational Rights and Privacy Act 34 CFR Part 99
- Electronic Communications Privacy Act of 1986 (ECPA)
- Idaho Code § 67-5745C(3)
- Idaho Code Chapter 1, Title 74 (Idaho Public Record Act)
- Idaho Technology Authority (ITA)
- Idaho State Board of Education (SBOE)
- University Statement of Shared Values
- University Policy 1140 (Copyright Fair Use)
- University Policy 1060 (Non-discrimination and Anti-harassment)
- University Policy 1065 (Sexual Harassment, Sexual Misconduct, Dating Violence, Domestic Violence, and Stalking)
- University Policy 2020 (Student Code of Conduct)

- University Policy 6120 (Payment Card Acceptance Policy)
- University Policy 7070 (Employee Political Activities)

1. Policy Purpose

To maximize the value of University IT resources and permit freedom to use such resources consistent with state and federal law and the policies of the Idaho Technology Authority (ITA) and the Idaho State Board of Education (SBOE).

2. Policy Statement

University IT Resources are provided to support Boise State University and its academic, research, and service missions; its business and administrative functions; and its student and campus life activities. Use of University IT Resources must comply with state and federal laws and regulations, executive orders, and policies of the Idaho Technology Authority (ITA), the Idaho State Board of Education, and University policies.

3. Definitions

3.1 Information Technology (IT) Resources

An array of products and services that collect, transform, transmit, present, and otherwise make data into usable, meaningful, and accessible information. IT Resources include but are not limited to desktop and laptop computers; tablets; handheld devices such as cell phones, e-mail, voicemail, servers, central computers, and networks; cloud storage systems; network access systems including wireless systems; portable hard drives and databases; computer software; printers and projectors; telephone equipment and switches including local and long-distance services; fax machines; camcorders; TVs; gaming systems and streaming devices; satellite equipment; and any other current or future IT resource adopted by the University.

4. Personal Limited Use

The primary purpose of University IT Resources is to conduct official University business. University employees may, however, use the University's IT Resources for de minimis personal use on their personal time provided such use does not violate any laws, regulations, or University policies.

5. Academic Freedom and Associated Responsibilities

a. The First Amendment rights of academic freedom and freedom of expression, including the responsibilities associated with those rights, apply to the use of University IT Resources.

b. These rights and responsibilities are guided by this policy, the University's Statement of Shared Values, University Policy 1060 (Non-discrimination and Anti-harassment), University Policy 2020 (Student Code of Conduct), other applicable University policies, the policies of the Idaho State Board of Education and Idaho Technology Authority (ITA), Executive Orders, and other state and federal laws and regulations.

6. Limited Privacy Expectations

Boise State University, as a public institution of higher education, is subject to the public records laws of the State of Idaho. While some information may be exempt from disclosure, information or records stored on University IT Resources are generally presumed to be open for review and inspection and are subject to public disclosure requests and examination by University officials in order to determine if exemptions apply to prohibit disclosure. The University will examine and disclose information or records stored on University IT Resources as required by law. In addition, the University may have a business necessity or reason to access and examine information, records, files, communications, and accounts of its employees or students, including but not limited to the investigation of substantiated complaints or other reliable evidence of misuse or violation of law or policy. Therefore, users of University IT Resources should have a limited expectation of privacy in the use of such resources.

7. Prohibited Actions

a. University IT Resources must not be used for:

- Engaging in commercial or personal profit-making purposes or for personal benefit where such use incurs a cost to the University and is not academic or work related.

- Accessing or attempting to access another person's directory, files, or mail, whether protected or not, without permission of the owner. Attempts to access unauthorized IT Resources via the computer network, to decrypt materials, or to obtain privileges to which the user is not entitled are prohibited.

- Visiting, viewing, or distributing Internet sites or materials that contain obscenity, as defined under applicable federal and state law; and publishing, displaying, transmitting, retrieving or storing such obscene material.

- Intentionally accessing or disseminating pornography by University employees, temporary staff, contractors or vendors, unless such use is specific to work-related functions and has been approved by the respective manager, or such use is specifically related to an academic discipline or grant/research project. This applies to any electronic communication distributed or sent within the University network or to other networks while using the University network.

- Intentionally or negligently interfering with the proper operation of any system or its use by others.

- Creating or distributing defamatory material or true threats, as defined under applicable law, or other illegal activity including but not limited to stalking as defined under applicable law.

- Downloading, disseminating, storing, using, or printing materials in violation of copyright laws including articles, music, videos, games, and software (see University Policy 1130 - Use of Copyrighted Works for more details.

- Causing congestion, overload, or disruption of networks or systems, including the distribution of chain letters.

- Creating or knowingly disseminating unwanted and unsolicited emails or materials (spam) in such a large volume that it tends to disrupt the proper functioning of University IT Resources or an individuals' ability to use such resources.

b. Users of University IT Resources must not:

- Remove, transfer, disable, or dispose of computer software licensed to the University. Contact the Office of Information Technology (OIT) for details.

- Share University user credentials and passwords with other individuals. Each user must have an individual account, passwords must be protected, and the user must not leave a University IT Resource logged on when not present unless the University IT Resource has been electronically locked and is in a secure area, such as a private office.

- Engage in excessive use of University IT Resources, such as when a user or process has exceeded established limits placed on the services, or when the user is consuming a resource to a level such that service to other users is degraded or where the actions of the user could cause degradation if the user is permitted to continue the practice or

activity. In such circumstances, the University may impose restrictions or limits on the use of the resource.

- Falsify e-mail or newsgroup postings.
- Try to circumvent login or security procedures.

8. Passwords and Accounts

a. All active faculty, staff, students, and affiliates of the University must have a unique username and password to access University systems and data.

b. Usernames are assigned to all active faculty, staff, students, and affiliates of the University and are generated automatically by University systems based on a combination of the individual's first and last name. After a user is considered inactive, their account will be deactivated, and they will be removed from the appropriate University systems. Standards for activity, username generation, and usage can be found on the OIT website.

c. Passwords are established by the individual and must be safeguarded. Standards for the rules and complexity of the password can be found on the OIT website.

9. 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. Use of University IT Resources is a privilege, not a right, and abuse may result in the immediate removal of privileges pending final resolution of the matter.

c. 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); or
- Referral to Human Resources for employee violations, which may result in discipline up to and including dismissal; and/or
- Exclusion from campus under University Policy 12020 (Exclusion from Campus); and/or

- Restricted access or loss of access to the University network or University IT Resources; and/or

- Civil and/or criminal liability.

10. Related Information

OIT Accounts and Access Information
https://www.boisestate.edu/oit/accounts/

Revision History

June 2004; January 2016; February 02, 2022