



BOISE STATE UNIVERSITY

University Policy 8000

Information Technology Resource Use

Effective Date

November 1997

Last Revision Date

August 14, 2025

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 (FERPA) 34 CFR Part 99
- Electronic Communications Privacy Act of 1986 (ECPA)
- Idaho Code Chapter 1, Title 74 (Idaho Public Record Act)
- Idaho Technology Authority (ITA) Policies
- University Statement of Shared Values
- University Policy 1020 (Public Records Management)
- University Policy 1060 (Non-discrimination and Anti-harassment)
- University Policy 1065 (Sexual Harassment, Sexual Misconduct, Dating Violence, Domestic Violence, and Stalking)
- University Policy 1110 (Conflict of Interest and Commitment)
- University Policy 1130 (Use of Copyrighted Works)
- University Policy 1160 (Solicitation)
- University Policy 2020 (Student Code of Conduct)

- University Policy 2250 (Student Privacy and Release of Information)
 - University Policy 4000 (Faculty Code of Rights, Responsibilities, and Conduct)
 - University Policy 6120 (Payment Card Acceptance Policy)
 - University Policy 7000 (Position Definitions)
 - University Policy 7070 (Employee Political Activities)
 - University Policy 7035 (Affiliates, Affiliate Faculty, and Volunteers)
 - University Policy 8060 (Information Privacy and Data Security)
 - University Policy 9030 (Antenna and Transmission Systems)
-

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).

2. Policy Statement

Boise State University IT Resources are provided to support the university's 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 Account

Access to University IT Resources granted by the university solely for a User's own use consisting of a username, derived from the individual's first and last name, and a password.

3.2 University Information Technology (IT) Resources

Technology belonging to the university that collects, processes, stores, and transmits data to create usable information, including but not limited to:

- a. Hardware
 - Desktop and laptop computers
 - Tablets and handheld devices (e.g., smartphones)
 - Servers, central computers, and network infrastructure

- Cloud storage systems (e.g., Infrastructure as a Service (IaaS), Software as a Service (SaaS), Platform as a Service (PaaS))
- Network access systems (wired and wireless)
- Printers, projectors, and other peripherals
- Telephone equipment and services
- Audio/visual recording equipment (e.g., cameras, microphones)
- Digital displays, televisions, and gaming systems
- Any other current or future technology adopted by the University

b. Software

- Operating systems and application software
- Software as a service (SaaS)
- Databases

c. Services

- Email, voicemail, and other communication tools
- Data storage and access services
- Network and system administration services
- IT support services

3.3 User(s)

Any individual, including but not limited to employees as defined for any position under University Policy 7000 (Position Definitions); students as defined under University Policy 2250 (Student Privacy and Release of Information); and affiliates, affiliate faculty, and volunteers as defined under University Policy 7035 (Affiliates, Affiliate Faculty, and Volunteers).

4. 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 ITA, Executive Orders, and other state and federal laws and regulations.

5. Limited Privacy Expectations

- a. 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 or transmitted 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 to determine if exemptions apply to prohibit disclosure.
- b. 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.

6. Acceptable Use

The primary purpose of University IT Resources is to conduct official University business. Users 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, University policies, or otherwise incur an additional cost to the university.

7. Unacceptable Use

Users must not use University IT Resources to/for:

- a. Commercial activities that are not for the purpose of or in support of pre-approved academic or University purposes.

- b. Personal gain, profit, or benefit, except where such usage is allowed under section 6 (Acceptable Use) and does not incur a cost to the university.
- c. Outside business, private employment, other activity for the benefit of a non-University entity or person unrelated to pre-approved academic or university purposes, or any other activity that violates University Policy 1110 (Conflict of Interest and Commitment) or University Policy 1160 (Solicitation).
- d. Political activity that is prohibited by University Policy 7070 (Employee Political Activities).
- e. Access or attempt to access another person's directory, files, or e-mail, whether protected or not, without permission of the owner.
- f. Attempt to access unauthorized University IT Resources, decrypt materials, or to obtain privileges to which the User is not entitled are prohibited.
- g. Visit, view, or distribute data or images that contain obscenity as defined under applicable federal and state law, or otherwise are in violation of University policies, standards, procedures, or codes of conduct. This also includes publishing, displaying, transmitting, retrieving, or storing such obscene material.
- h. Intentionally store, access, or disseminate pornography, unless such use is specific to work-related functions, including academic pursuits, conducting research for a sponsored project, or conducting a University investigation, and such use has been approved in advance by the respective manager.
- i. Engage in illegal activity (e.g., copyright infringement, defamation, threats of violence, harassment, stalking, and other illegal actions) as defined by applicable law (e.g., trademark law, export control law).
- j. Create or knowingly disseminate unwanted and unsolicited emails or materials (spam) in such a large volume that it disrupts the proper functioning of University IT Resources or an individual's ability to use such resources.
- k. Intentionally or negligently interfere with the proper operation of University IT Resources by physical or technological means (e.g., propagation of harmful software, denial of service attacks, etc.).

Users of University IT Resources must not:

- a. Use their Boise State credentials to register for or access non-University IT Resources which are in no way related to their relationship with the University (e.g., use their University email address to register for a personal streaming service account).
- b. Share their Boise State credentials.
- c. Circumvent login or security procedures.
- d. 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.
- e. 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 University IT Resource.
- f. Falsify electronic records or communications.
- g. Enter any sensitive, restricted, or otherwise protected data into any generative AI tool or service.

8. User Data Storage and Account Termination

Account termination refers to the criteria used for determining User Account disabling, termination, deletion, and removal. This also includes the User Account being removed from all groups and permissions. Once an Account has been removed, the Account may be reassigned to the original owner of the Account upon their return to the university.

8.1 Affiliate Accounts

Access to Accounts and IT systems will be automatically terminated after twelve (12) months. Early termination or extensions to this timeframe must be requested from the OIT Help Desk, approved, and documented.

8.2 Employee Accounts

This section does not apply to adjunct faculty account access (see section 8.3) and employees

separating with emeritus status account access (see University Policy 4280 - Emeritus Faculty and University Policy 7480 - Emeritus Classified and Professional Employees).

- a. Access to Accounts and University IT Resources will end on the last day of employment, at which time the Account will be deactivated, and all access to the appropriate University systems will be removed.
- b. If the employee is both staff and adjunct faculty, upon the employee's separation from their staff role, an Employee Separation Form must be completed so that access pertaining to the employee's staff role can be removed.
- c. The supervisor may request the transfer of University IT Resources to another employee prior to the departure of the separating employee.
- d. If the separating employee's University IT Resources are not transferred to another employee, OIT will:
 - Move the contents of the separating employee's Google Drive to a folder in the manager's Google Drive (This excludes files and folders in a Google Shared Drive that belong to a team and are owned by the university and not the individual. Files and folders in a Google Shared Drive remain even if the employee leaves the university and their Account is deleted).
 - Move the contents of the separating employee's H: drive (i.e., a network share on a Microsoft server that contains a User's home directory) to a folder in the manager's H: drive.

8.3 Adjunct Faculty Accounts

Upon termination of an adjunct faculty, the appropriate department administrator must contact Human Resources and Workforce Strategy at <https://www.boisestate.edu/hr/> to initiate the Account termination process.

8.4 Student Accounts

Students and student applicants will retain access to their Student Google Workspace and University email Account until they are identified for deactivation following the criteria below. International students will retain access to their account as needed to comply with the University's Student And Exchange Visitor Information System (SEVIS) reporting and record maintenance requirements.

- Newly admitted students who enrolled but dropped all their courses prior to the start of the term.

- One year after completion of a degree or certificate, or end of active or registered enrollment activity.

9. Policy Non-Compliance

- a. Suspected violations of this policy must 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 under the Student Code of Conduct (University Policy 2020); or
 - Referral to Human Resources and Workforce Strategy 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/>

University Policy 4280 (Emeritus Faculty)

University Policy 7480 (Emeritus Classified and Professional Employees)

Revision History

June 2004; January 2016; February 02, 2022; August 01, 2024; August 14, 2025