30.12 - Acceptable Use of Technology Resources

Owner:

- **Position:** Information Technology VP and Chief Information Officer
- **Name:** Dan Ewart
- **Email:** dewart@uidaho.edu

Last updated: July 01, 2022

Contents:

A. Purpose. The University of Idaho (U of I) provides access to technology resources and assets in order to support its land grant mission in all areas. These include instruction, research, outreach, and service missions; administrative functions; and student and campus life activities. This policy sets forth the rights and responsibilities of users of U of I technology resources. It also defines or links to examples of measures that may be taken by the institution to ensure the integrity of U of I resources and compliance with applicable law and policy.

B. Scope. This policy applies to all users of U of I technology resources, whether they are formally affiliated with U of I and whether they are accessing them on a U of I campus or using them from other locations.

C. Definitions

C-1. Technology Resources. All university owned, operated, leased, or contracted technology, including but not limited to:

- Computing, networking, telecommunication, storage, and information resources.
- All information maintained within the university's computing resources.
- All technology resources including all hardware, software, applications, databases, and storage media.

C-2. Data Owner. The unit administrator with direct responsibility for all access and use of designated types of data. Use of this term, in connection with this policy, shall not affect university claims or rights of ownership of data or ownership of third-party data in the possession of the university.

D. Policy. The University of Idaho provides access to and use of its technology resources to its students, staff, faculty, and others, as part of its business practices that, in turn, support its mission. Access and use of U of I technology resources is a privilege and requires that users of such technology resources act responsibly, regardless of ownership of the end point computing device used to access these resources. Users shall only access or use U of I

technology resources in a manner that is consistent with applicable federal and state laws and Idaho State Board of Education and U of I policies and procedures. Applicable laws and policies are not limited to those specifically addressing access to and use of computers and networks; they may also include, but are not limited to, laws and policies related to personal conduct as reflected in the U of I Faculty Staff Handbook and other university policies. Users accessing U of I technology resources have no expectation of privacy with respect to the use of U of I technology resources.

D-1. User Responsibilities. Users of U of I technology resources must:

a. Follow all U of I policies and procedures and IT standards.

b. Actively maintain the security of all devices accessing U of I technology resources or being used to access, store, or process U of I-maintained data.

c. Actively maintain the security and privacy of university data or U of I-maintained third-party data and store or process such data only in authorized locations, consistent with U of I policies and standards.

d. Report privacy, security, or technology policy violations to the U of I OIT Security Office using the OIT Support Portal or security@uidaho.edu.

D-2. User Actions Constituting Misuse of U of I Technology Resources. The actions described below shall be considered misuse of U of I technology resources:

a. Utilizing any identity or account not specifically assigned by U of I to the user.

b. Hindering, monitoring, or intercepting another user's network traffic, except as expressly authorized as an exception to this policy (See section F).

c. Attempting to access, disclose, destroy, use, or modify university systems or data without authorization of data owners.

d. Using technology resources for the creation or transmission of materials which may put any person's personal safety at risk;

e. Using technology resources for unauthorized access to any system or network.

f. Using technology resources for unlawful communications or activity, including threats of violence, obscenity, child pornography, defamation, harassing communications (as defined by law) such as cyberstalking or other similar activities in violation of stalking laws.

g. Engaging in the unauthorized copying, distributing, or transmitting of copyrighted materials such as software, music, or other media. See FSH 5300 Copyrights, Protectable Discoveries and Other Intellectual Property Rights.

h. Using technology such as traffic anonymizers, proxy services, or third-party VPN that disguise country of location while accessing U of I technology resources, except as expressly authorized as an exception to this policy (see section F).

i. Using technology resources or applications to provide an unauthorized gateway or access point in or out of any U of I networks.

j. Using or accessing technology resources from unauthorized non-US locations, including those limited by Export Control, trade sanctions , or other laws, regulations, or University policy. See APM 45.19 U.S. Export Controls, APM 70.23 University International Travel, and FSH 3250 Flextime/Flexplace.

k. Using technology resources for partisan political or campaign activities, such as participating or intervening in a campaign for public office or making technology resources available to a candidate, campaign, political party, or political actions committee. See FSH 6230 Political Rights of University Employees and FSH 3170 University Ethics section B-10.

l. Using technology resources for commercial purposes (including but not limited to personal financial gain), except as allowed by FSH 3260 Professional Consulting and Additional Workload.

m. Using university resources for personal, non-commercial purposes, excluding uses such as personal email or access to the internet, when such activities do not interfere with an individual's employment responsibilities at UI or give rise to a cost to U of I.

E. Noncompliance. The U of I may take any actions it deems necessary to protect and manage the security and integrity of its technology resources. Noncompliance with this policy may result, depending upon the nature of the noncompliance, in the user's account or access to U of I technology resources being temporarily suspended, disabled, or permanently terminated. In the case of temporary suspension, U of I may require implementation of remedial measures or satisfaction of educational courses prior to reinstatement of the user's account or access. Additionally, the user may be referred for institutional sanctions to the appropriate university disciplinary body and may be subject to civil and criminal penalties.

F. Exceptions. Sections D-2.k through D-2.m do not apply to students, guests, or residents in university housing except when such uses are in violation of federal or state law, or give rise to a cost to U of I. Requests for other exceptions to this policy may be submitted through the OIT Support Portal. The U of I Information Security Officer will assess the risk and make a recommendation to the U of I Vice President for Information Technology and Chief Information Officer.

G. Contact Information. The OIT Information Security Office can assist with questions regarding this policy and related standards. Please submit your question on the OIT Support Portal.

H. References.
NIST – SP 800-171 revision 2
U of I – FSH 2300 –Student Code of Conduct
U of I – FSH 2400 – Disciplinary Process for Alleged Violations of Student Code of Conduct
U of I – FSH 3170 – University Ethics
U of I – FSH 3250 – Flextime/Flexplace
U of I – FSH 3260 – Professional Consulting and Additional Workload
U of I – FSH 5300 – Copyrights, Protectable Discoveries and Other Intellectual Property Rights
U of I – FSH 5700 – Research Data
U of I – APM 30.11 – University Data Classification and Standards
U of I – APM 45.19 – Export Controls, U.S.
U of I – APM 65.02 – Records Inventory, Retention and Disposition
U of I – APM 65.06 – University Electronic Records Management Guidelines
U of I – APM 70.23 – University International Travel
U of I – Approved Storage Locations

Version History

Amended 2022. Comprehensive review and revision, including language to address new technologies to disguise a person's location.

Amended 2017. Substantially revised to address responsibilities of users and systems without being specific to frequently changing types of technology resources.

Adopted 2007.