**Preamble:** The University of Idaho (UI) provides access to technology resources in order to support its 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 UI technology resources and the measures that may be taken by the institution to ensure the integrity of UI technology resources and compliance with applicable law and policy.

**Contents:**
A. Definitions
B. Policy
C. Scope
D. Exceptions
E. Process/Procedure
F. Contact Information
G. References

A. Definitions.

**A-1. Technology resources**
- All University owned, operated, leased, or contracted computing, networking, telecommunication, and information resources;
- All information maintained within the University’s computing resources;
- All voice and data networks, telecommunications and communication systems and infrastructure; and
- All technology resources including all hardware, software, applications, databases, and storage media.

**A-2. Data owner.** The senior university college/division/departmental executive 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.

**B. Policy.** UI provides access to and use of its technology resources to its students, staff, faculty, and others, in order to support its mission. Access and use of UI technology resources is a privilege and requires that users of such technology resources act responsibly. Users shall only access and/or make use of UI technology resources in a manner that is consistent with applicable federal and state laws and Idaho State Board of Education and UI policies and procedures. Users accessing UI technology resources have no expectation of privacy with respect to such uses. Please note that 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. (See FSH 3170 B-7)
B-1. User Responsibilities. Users of University of Idaho technology resources must:
   a. Follow all applicable federal and state laws;
   b. Follow all UI policies and procedures and IT standards;
   c. Actively maintain the security of all devices accessing UI technology resources or being used to access, store, or process UI-maintained data.
   d. Actively maintain the security and privacy of university data or UI-maintained third party data and store such data only in authorized locations, consistent with UI policies and standards.
   e. Report privacy, security, or technology policy violations to the UI ITS Security Office.

B-2. User Actions Constituting Misuse of UI Technology Resources. User actions, such as those described below, of University of Idaho technology resources shall be considered misuse of UI technology resources:
   a. Utilizing any identity or account not specifically assigned by UI to the user;
   b. Hindering monitoring, or intercepting another user’s network traffic, except as expressly authorized by the UI;
   c. Attempting to access, disclose, destroy, use, or modify university systems or data without authorization of data owners;
   d. Using technology resources for partisan political or campaign activities (see FSH 6230), 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 also FSH 3170 B-10).
   e. Using technology resources for commercial purposes (including but not limited to personal financial gain)
   f. Using university resources for personal, non-commercial purposes, excluding uses such as checking of 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 UI.
   g. 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;
   h. Using technology resources for the creation or transmission of materials which may put any person’s personal safety at risk;
   i. Using technology resources for unauthorized access to any system or network;
   j. Engaging in the unauthorized copying, distributing, or transmitting of copyrighted materials (see FSH 5300), such as software, music, or other media.

B-3. Noncompliance. Non-compliance with this policy may result, depending upon the nature of the non-compliance, in the user’s account or access to UI technology resources being temporarily suspended or disabled or permanently terminated. In the case of temporary suspension, UI may require implementation of certain remedial measures or satisfaction of certain 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.

**B-4. Remediation.** The University may take any actions it deems necessary to protect and manage the security and integrity of its technology resources, including but not limited to temporarily suspending or disabling user accounts or limiting the available resources through traffic shaping, data caps, or other measures.

**C. Scope.** This policy applies to all users of University technology resources, whether or not formally affiliated with UI and whether on a UI campus or accessing and using technology resources from remote locations.

**D. Exceptions to the Policy.** Sections B-3(d-f) 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 UI.

Other exceptions to this policy may be submitted in writing to the UI Information Security Officer who will assess the risk and make a recommendation to the UI-CIO.

**E. Process/Procedure/Standards.** Given the changing nature of technology, users are encouraged to regularly review the latest IT standards on the ITS website for specific guidance on acceptable uses of technology resources.

**F. Contact Information.** The ITS Information Security Office (its-security@uidaho.edu) can assist with questions regarding this policy and related standards.

**G. References.**

- Federal Information Security Management Act (FISMA) - National Institute of Standards and Technology (NIST) SP-800-53, Revision 4
- UI - FSH 2300 – UI Student Code of Conduct
- UI - FSH 3170 – University Ethics
- UI - FSH 5300 - Copyrights, Protectable Discoveries and Other Intellectual Property Rights
- UI - FSH 5700 – Research Data
- UI – APM 30.11 - University Data Classification and Standards
- UI - APM 45.19 - Export Controls, U.S.
- UI – APM 65.02 - Records Inventory, Retention and Disposition
- UI – APM 65.06 - University Electronic Records Management Guidelines