**POLICIES AND PROCEDURES**

**Information Technology Services**

**Acceptable Use**

**ISUPP 2400**

*POLICY INFORMATION*
**Policy Section:** *Information Technology Services*
**Policy Title:** *Information Technology Services Acceptable Use*
**Responsible Executive (RE):** *Chief Information Officer*
**Sponsoring Organization (SO):** *Information Technology Services*
**Effective Date:** *TBD, March 28, 2016*
**Revised:** *TBD, August 15, 2018; May 4, 2018*
**Review Date:** *December 2030*

## I. INTRODUCTION

This policy outlines the acceptable use of the University's Information Technology (IT) resources, including computers, networks, email, internet access, software, and other technology-related services. The goal of this policy is to ensure that all users have access to a secure, reliable, and fair computing environment, while maintaining the integrity of the University's systems and adhering to legal and ethical standards.

## II. DEFINITIONS

A. Adequate Cause. One or more acts or omissions which, singly or in the aggregate, have directly and substantially affected or impaired an employee's performance of his or her assigned duties or the interests of the Board or University. In addition, any conduct seriously prejudicial to the Board or University may constitute Adequate Cause for discipline up to and including dismissal or termination of an employee.

B. Chief Information Security Officer. The ISU employee that is responsible for leading information security activities at ISU.

C. Critical Information. Information identified by applicable laws, regulations or policies as personal information, individually identifiable health information, education records,

personally identifiable information, non-public personal or institutional data, confidential personal information, or sensitive scientific or sponsored project information.

D. Digital Trespass. Digital trespass includes any intentional or unintentional activity that exceeds the level of access granted to a User, circumvents security controls, invades another User's digital workspace, or attempts to access, alter, disrupt, or monitor systems, services, data, or accounts without proper authorization.

E. Employee. Any individual employed by the University in any capacity as defined in ISUPP 3050: *Categories of Employees*.

F. Information. An electronic data set that is considered valuable to an organization. Information is classified in the *Information Technology Services Asset Management ISUPP 2430*.

G. Institutional Information. Information used for the purpose of conducting University business the disclosure, alteration, or destruction of which could result in a moderate level of risk to the University. Information that is not explicitly classified as Critical Information or Public Information should be treated as Institutional Information.

H. IT System. ISU's data processing hardware, software, data transmission equipment and infrastructure, data storage devices, and the electronic information stored, processed, or transmitted via these components (including electronic mail).

I. Secure. The state in which a device or system is effectively protected against unauthorized access, use, disclosure, alteration, or destruction. To be considered "Secure," a device must implement approved technical and organizational safeguards—including, but not limited to, encryption, strict access controls, and regular risk assessments to ensure the confidentiality, integrity, and availability of the data it contains.

J. Sensitive data. Any information that is not public is considered Sensitive. Both Institutional and Critical Information are Sensitive Information.

K. Users. Any individual who accesses, attempts to access, interacts with, transmits, receives, stores, or otherwise utilizes University information technology resources. This includes, but is not limited to, students, faculty, staff, affiliates, contractors, volunteers, visiting researchers, third-party service providers, automated processes, guests, and any other entity granted explicit or implicit authorization to use University systems, networks, data, or services.

## III. POLICY STATEMENT

ISU will ensure the confidentiality, integrity, and availability of its IT System while supporting academic freedom and general access for the campus community. This policy applies to all University IT resources whether owned, leased, managed operated, or otherwise authorized for use

by the University. This policy applies to all Users of the University's IT resources, including students, faculty, staff, contractors, guests, and any other individuals or entities granted access to the University's computing systems regardless of location and access method. Unless otherwise restricted, personally owned devices that are used to access University systems or data are considered in scope and are subject to this policy. The University will maintain systems to support the secure and effective use of IT resources. Inappropriate use of resources by Users exposes the University to risk. Unauthorized access to, or interference with, University Information Technology resources, including Digital Trespass, is strictly prohibited. Violations of this policy may result in loss of access privileges, disciplinary action, termination of employment or enrollment, and referral to law enforcement where appropriate.

## IV. AUTHORITY AND RESPONSIBILITIES

A. All Users are responsible for ensuring that their actions comply with applicable University policies, contractual obligations, and local, state, and federal laws and for protecting information, data, and the University's IT Systems.

B. Chief Information Officer (CIO). Serves as the appellate authority for decisions made under this policy and provides final administrative review of disputes, exceptions, or sanctions related to IT resource use.

C. Chief Information Security Officer (CISO). Oversees the security, integrity, and availability of University information systems, including implementation of security controls, incident response coordination, risk assessments, and enforcement of relevant information security standards.

D. Information Technology Services. Maintains, repairs, and supports University IT systems and infrastructure; manages system availability; and implements technical measures required to enforce this policy. The IT department also provides support, training, and necessary tools to help Users comply with this policy.

E. Human Resources. Address staff and employee violations through corrective action, performance management, or disciplinary processes, consistent with University policy and applicable employment agreements.

F. Public Safety. Investigates allegations of misuse of University IT resources when appropriate and coordinates with external law-enforcement agencies.

G. Dean of Students. Administers student conduct processes and applies disciplinary action for student violations of this policy, consistent with the Student Code of Conduct.

## V. PROCEDURES TO IMPLEMENT

A. User Responsibilities.

1. Primary Use and Limits. IT resources exist to support the University's mission and should be used principally for:
    a. Academic use;
    b. Instruction and instructional support;
    c. Research and creative activities;
    d. Administrative functions;
    e. Healthcare operations as regulated under additional University policies; and,
    f. Limited personal use that does not conflict with law, policy, resource availability, or the primary purposes stated above.
2. Security. Users must take reasonable precautions and comply with all University defined security standards and configuration requirements applicable to the systems and services they access. Users are responsible for ensuring the security and confidentiality of their accounts and data. This includes using strong passwords, not sharing credentials, and logging out when finished with a session.
3. Users must comply with all applicable federal and state laws as well as University policy on recording, privacy and electronic communications.
4. Privacy. Users should respect the privacy of others and handle sensitive information appropriately.
5. Protecting Devices. Users have a responsibility to secure any device that is used to access University owned systems. Users must not disable security controls on University managed devices. Users must also ensure the physical protection of devices from theft, loss, damage, and access by unauthorized individuals.
6. Reporting Issues: Users must promptly report any actual or suspected theft, loss, or damage of University IT resources. Users must also report any IT security incidents, breaches, or suspicious activities to the University's IT Helpdesk or Information Security office without delay.
7. Access Control. Users shall not attempt to gain unauthorized access to systems or data, see ISUPP 2410 *Information Technology Services Access Control*. Any discovered vulnerabilities must be reported to the IT security team, not exploited.
8. Data Protection. Users must comply with all University data protection policies, including the secure storage, transmission, and disposal of sensitive data. Individuals shall not share their username or password nor allow others to use their accounts.

B. Communication. All opinions, advice, services, and other information expressed using ISU's IT System resources must be clearly presented as those of the individual and not representing the views or position of ISU unless acting in an official capacity, within the limits of one's authority. Employees may not utilize ISU's IT System for political lobbying.

C. Unacceptable Use of IT Resources.

1. The following activities are strictly prohibited:

a. Unauthorized Software and Services: include software and services that are licensed outside of ISU's IT systems but have not been reviewed, approved and deployed in accordance with ITS policies and University contract approval processes.

i. Users are prohibited from installing or using unauthorized software, including pirated software or programs that could harm the integrity of the system.

ii. Only software legally licensed for use on ISU's IT System may be installed or used.

iii. Software shall not be installed onto ISU's IT System in such a manner that its usage exceeds the actual number of purchased licenses, nor violates the vendor's terms and conditions for acceptable use.

iv. Users may not use unapproved external cloud services, applications, or platforms to store, process, or transmit University data.

b. Illegal Activities. Using IT resources for illegal purposes, including but not limited to copyright infringement, fraud, or unauthorized access to data, systems, or networks.

c. Harassment and Discrimination. Using IT resources to engage in harassment, bullying, hate speech, or any behavior that could create a hostile or discriminatory environment in violation of other applicable ISU policies.

d. Malicious Behavior.

i. Using IT resources to engage in Digital Trespass.

ii. Deliberately introducing malicious software (viruses, worms, etc.), unauthorized system access, or tampering with systems or data.

iii. Willfully create or propagate any virus, worm, Trojan or other destructive program code, unless each of the following conditions are met:

1. The activity is for academic / research purposes;

2. The activity takes place in an approved controlled environment;

3. The virus, worm, Trojan or other destructive program code is not propagated; and,
4. The activity has been specifically approved in advance, and in writing, by the University's Chief Information Security Officer.

iv. Exploiting vulnerabilities or deficiencies in ISU's IT System to damage systems or information, to obtain access to resources beyond those they have been authorized to obtain, to engage in Digital Trespass, or to remove resources from other individuals without authorization.

v. Testing or attempting to compromise internal controls unless this activity is specifically approved in advance, and in writing, by the Chief Information Security Officer.

e. Inappropriate Content.

i. Accessing, storing, or transmitting obscene, sexually explicit, or otherwise offensive material.

ii. Requesting, viewing, distributing, or storing obscene or pornographic material unless the respective Vice President approves in writing and such use is specifically related to an academic discipline or grant/research project.

iii. Users who become aware of potential violations involving obscene or pornographic material must report it to the manager of their administrative or academic unit immediately.

iv. Incidents that may involve the administrative or academic manager should be reported to the appropriate Vice President or the Chief Information Officer.

v. Willful failure to report such a potential violation will be considered Adequate Cause and may result in sanctions.

f. Excessive Resource Consumption.

i. Engaging in activities that excessively burden the network or degrade performance, such as running programs that waste resources, engaging in unauthorized data scraping, or initiating distributed denial-of-service (DDoS) attacks.

ii. Users should be mindful of excessive printing and other high-resource activities. Use IT resources in a way that minimizes waste.

g. Impersonation. Misrepresenting the identity of the User, manipulating the appearance of communication or using manipulated or synthetic media to mislead others.

h. Copyrighted Material. Individuals may not use ISU's IT System to perform activities that illegally infringe on copyrighted material. This includes, but is not limited to, unauthorized copying, distribution, and/or use of copyrighted materials.

i. Intellectual Property and Licensing. Users may not infringe on intellectual property rights or violate licensing, patent, or trademark protections. This includes, but is not limited to, software piracy; use of unlicensed or improperly licensed software; circumvention of digital rights management (DRM) controls; and any activity that breaches contractual terms governing access to digital resources.

j. Commercial Use. Individuals may not utilize ISU's IT System to engage in unauthorized commercial actions including, but not limited to, running a business or running advertisements of businesses.

D. Enforcement and Sanctions

1. Users should have no expectation of privacy when using University IT resources. The University reserves the right to monitor, log, review and audit IT usage to ensure compliance with this policy and safeguard the University's resources.
2. Violations of this policy may result in disciplinary action (defined further below), including suspension or termination of IT access, and in serious cases, legal action.
3. Disciplinary Actions. Available disciplinary actions include, but are not limited to:
    a. Students: Violations may lead to academic discipline, including warnings, suspension, or expulsion as per the Student Code of Conduct.
    b. Employees: Violations by faculty or staff may lead to disciplinary actions, including but not limited to warnings, suspension, or termination, in accordance with University policies.
    c. Others: Contractors, visitors, and external users found in violation of this policy may be denied access, have their access revoked, and may face legal consequences.

E. Acceptable Use Agreement

1. Individuals authorized to use ISU's IT Systems are expected to abide by ethical and legal standards at all times, be responsible for their own behavior, and comply with ISU's policies and procedures.
2. Users will be asked to acknowledge their agreement before being granted access to University Information Technology Systems and periodically thereafter (see attached *Acceptable Use Agreement*).

## VI. REFERENCES

A. Idaho State Board of Education Policy II.L(3) Adequate Cause

*B.* ISUPP 1110 *Equal Opportunity and Prohibition of Discrimination, Harassment, and Retaliation*

C. ISUPP 1120 *Title IX Sexual Harassment: Stalking, Sexual Assault, and Intimate Partner Violence*

D. ISUPP 2410 *Information Technology Services Access Control*

E. ISUPP 2430 *Information Technology Services Asset Management*

F. ISUPP 2460 ITS *Compliance and Sanctions*

G. ISUPP 2470 *Electronic Messaging*

H. ISUPP 2490 *ITS Incident Management*

I. ISUPP 3050 *Categories of Employees*

## VII. ATTACHMENTS

Acceptable Use Agreement

Idaho State University

# Acceptable Use Agreement

**By being given a username and password granting me access to ISU's data processing hardware; software, data transmission equipment and infrastructure; data storage devices; and the electronic information stored, processed, or transmitted via these components (hereafter referred to as ISU's IT System) I agree to abide by the following guiding principles:**

## Confidentiality

**I agree to maintain confidential access to all ISU IT System resources to which I am given access and to accept full responsibility for any activity performed via my ISU IT System account.** All ISU IT System accounts are nontransferable and each individual must obtain separate and unique access. Passwords must remain private and cannot be shared. Service Accounts shall only be shared with authorized account Users.

## Integrity

**I will not use my access to ISU's IT System resources for personal gain, in violation of ISU's security policies, or to otherwise compromise the integrity of ISU's IT System.** Legitimate use of an ISU IT System account does not extend to whatever I am capable of doing with it. Although some rules are built into the system itself, these restrictions cannot limit completely what I can do and can see. In any event, I am responsible for my actions whether or not rules are built in, and whether or not I can circumvent them. Misuse includes (but is not limited to): unauthorized access to or usage of ISU's IT System; unauthorized use or sharing of account passwords; unauthorized alteration or use of another individual's program(s) or file(s); and knowingly attempting to circumvent established security policies and procedures.

## Protection

**I will take reasonable care of all ISU IT resources to which I am granted access, protecting them from unnecessary wear, damage, or abuse.** Because ISU's IT System is a shared environment, I agree to use my access in a manner that does not interfere with the work of others. I will treat all University owned equipment with care and respect, as it remains the property of the University and must be returned to the University. I will secure devices physically when they are not in use and report any damage, loss, or theft of equipment immediately to the IT department. I will not lend company equipment to others, including family members. I will follow all instructions for the proper handling and storage of equipment, especially when working outside the office premises.

## Copyrighted Material

**I will not download, share and/or distribute copyrighted materials without the permission of the copyright holder.** Idaho State University does not own much of the computer software in use on campus. Instead, the University obtains licenses for the use of computer software from a variety of outside sources. Neither faculty nor staff has the right to reproduce it unless authorized.

## Policies and Procedures

Terms of acceptable behavior found in the Information Technology Policies also apply. Any violation of acceptable behavior as defined in these policies and procedures may also be considered a violation of this Agreement.

**I agree to use ISU's IT System solely for University instructional, educational, research, administrative, healthcare, or authorized personal use activities. I further acknowledge that any abuse of this agreement may result in the loss of my computer privileges, suspension and/or dismissal, disciplinary action, or legal action.**