Idaho State University

# POLICIES AND PROCEDURES

## Information Technology Services

## Acquisitions, Development, and Maintenance

## ISUPP 2420

*POLICY INFORMATION*
**Policy Section:** *Information Technology Services*
**Policy Title:** *Information Technology Services Acquisitions, Development, and Maintenance*
**Responsible Executive (RE):** *Chief Information Officer*
**Sponsoring Organization (SO):** *Information Technology Services*
**Dates: Effective Date:** *March 28, 2016, TBD*
**Revised:** *May 4, 2018, TBD*
**Review Date:** *May 2031*

## I. INTRODUCTION

Idaho State University relies on information technology systems, services, and applications to support its academic, research, clinical, and administrative functions. Effective stewardship of these resources is essential to ensure their reliability, security, accessibility, and alignment with institutional priorities. This policy establishes the framework for the acquisition, development, maintenance, and lifecycle management of University information technology systems and services. It provides guiding principles to promote fiscal responsibility, reduce risks, encourage interoperability, and ensure that technology investments support the University's mission while complying with applicable laws and regulations.

## II. DEFINITIONS

A. Chief Information Officer (CIO). The ISU executive in charge of Information Technology Services.

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

C. Critical Information. Information required by applicable laws, regulations or policies to be kept confidential, such as personal information, individually identifiable health information, education records, personally identifiable information, non-public personal or institutional data, personal information, or sensitive scientific or sponsored project information.

D. Essential Computing Resources. Shared computing resources which cannot undergo loss of access for more than twenty-four (24) hours without causing unacceptable consequences due to a break in business continuity.

E. Information. A data set that is considered valuable to an organization.

F. Information System. A computing device that stores, processes, or transmits ISU Information.

G. 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.

H. Risk Assessment. A repeatable process for determining information security risk.

I. Third Parties. Visitors, contractors, volunteers etc. who need access to ISU's IT System.

## III. POLICY STATEMENT

Idaho State University requires that all information technology systems, services, software, and related equipment acquired, developed, implemented, or maintained by any University unit be reviewed and managed in accordance with established Information Technology Services (ITS) standards, procedures, and governance processes. All University employees, departments, and affiliated units must coordinate with ITS to ensure that technology acquisitions and projects meet security, accessibility, and data-protection requirements, and follow approved procurement, development, and maintenance practices. No information technology resource may be purchased, deployed, or materially modified without adherence to this policy. This policy applies to all University-administered technology resources regardless of funding source or location.

## IV. AUTHORITY AND RESPONSIBILITIES

A. Chief Information Officer. Provides final administrative review of disputes, exceptions, or sanctions related to IT resource use. Serves as the appellate authority for decisions made under this policy.

B. Chief Information Security Officer. 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 including waivers, when necessary.

C. Information Technology Services. Charged with overseeing Information Systems acquisitions and ensuring that all Systems are appropriately acquired, developed, and maintained.

D. Users. All members of the ISU community, including faculty, staff, volunteers, contractors, and visitors are responsible for protecting Information and the IT System.

## V. PROCEDURES TO IMPLEMENT

A. Security Requirements Analysis and Specification

1. The list of requirements for all IT System acquisitions will include security control requirements.
2. Information Systems technology will not be deployed to store, process, or transmit Critical Information unless the same technology is widely used and is generally accepted as stable, reliable, fit for its intended purpose and protects the confidentiality of the Critical Information. Where applicable, Information Systems technology must comply with statutory and regulatory requirements.
3. Prior to deploying Cloud applications which store, process, or transmit Critical or Institutional data, Users must receive approval from the CISO. Forms used to request permission are found on the University's Purchasing Services website (see also ISUPP 2570 *Purchasing Card*).
4. Mission critical hardware and software, or hardware used to store, process, or transmit Critical Information, must be purchased, rented, leased, or otherwise obtained from a CISO approved vendor who is able to provide both maintenance services and warranties.

B. Correct Processing in Applications

1. All Essential Computing Resources will be analyzed prior to acquisition for proper data input validation, proper data output validation, and proper processing of data.
2. Every information system module or utility that will clearly not be used and is not necessary for the operation of other essential systems software, must be removed or otherwise disabled prior to the system processing live or operational data.

C. Encryption

1. Cryptographic Controls
    a. All electronic Critical Information will be encrypted when in transit or at rest.
    b. All cryptographic keys will be stored and managed in a manner that prevents unauthorized modification, loss, and destruction.
2. Encryption Standard
    a. Only community and industry accepted ciphers and algorithms that are considered unbreakable will be utilized on ISU Information Systems (internally developed ciphers or algorithms are prohibited).
    b. Encryption keys will contain a minimum 128-bits.
    c. All ISU-owned equipment will implement the ITS employed malware protection solution.

D. Security of System Files

1. Operating systems on Essential Computing Resources will be configured according to the vendors' standard configuration guidelines or industry accepted standard configuration guides.

E. Security in Development and Support Processes

1. A formal change control process (and supporting documentation system) will be followed while implementing changes to Essential Computing Resources.
2. Testing of changes to Essential Computing Resources will occur prior to implementation and verification of the changes will occur following implementation.
3. Fixed passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, computers without enforced access control mechanisms, or in other locations where unauthorized persons might discover or use them.
4. A Risk Assessment will be performed and documented for all IT System resources that store or cache Critical Information to determine if data leak prevention controls should be applied or if other security controls negate the need for data leak prevention.
5. Outsourcing development of applications running on Essential Computing Resources will be properly supervised, monitored, and documented to ensure adherence to industry best practices and ISU information security policies.

F. Technical Vulnerability Management

1. All operating system and application software will be scanned regularly for known vulnerabilities, and any critical risks identified will be remediated within thirty (30) days, if possible.

2. All operating system and application software will be kept at a vendor supported, stable release level. Once a vendor discontinues security support for a given product, that product may no longer be used nor connected to ISU’s IT System.
3. Initial Information Systems set-up will be done through established University security protocols.
4. Users must not accept any form of assistance or software to improve the security of their computers without approval by the CISO.

G. Any deviations from this policy reasonably believed to be necessary must be approved in advance by the CISO. If the CISO denies the waiver, the decision of the CISO can be appealed to the CIO. The CIO’s decision is final.

## VI. RELATED LAWS AND POLICIES

A. ISUPP 2430 *Information Technology Services Asset Management*

B. ISUPP 2470 *Information Technology Services Electronic Messaging*

C. ISUPP 2520 *Information Technology Services Risk Management*

D. ISUPP 2560 *Purchasing*

E. ISUPP 2570 *Purchasing Card (PCard)*