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*
Revised: *May 4, 2018*
Review Date: *May 2021*

I. INTRODUCTION

It is the objective of Idaho State University (ISU) to ensure that security is an integral part of an Information System's life cycle.

II. DEFINITIONS

A. **Chief Information Officer:** The ISU executive in charge of Information Technology Services.

B. **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.

C. **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.

D. **Information:** A data set that is considered valuable to an organization. Information is classified in the *Information Technology Services Asset Management ISUPP 2430*.

E. **Information Security Manager:** The ISU employee that is responsible for leading information security activities at ISU.

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, see *Information Technology Services Electronic Messaging ISUPP 2470*).

H. **Risk Assessment:** A repeatable process for determining information security risk (see *Information Technology Services Risk Management ISUPP 2520*).

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

III. POLICY STATEMENT

Idaho State University requires that IT System resources be acquired, developed, maintained, and replaced in such a manner as to provide appropriate confidentiality, integrity, and availability for the life of the product.

IV. AUTHORITY AND RESPONSIBILITIES

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

The Information Technology Services department is charged with seeing that all Information Systems are appropriately acquired, developed, and maintained.

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 this same technology is widely used and is generally accepted as stable, reliable, and fit for its intended purpose.
3. 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 trusted and well-established vendor who is able to provide both maintenance services as well as 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 being used to process production vs. test data.

C. Encryption
   1. Cryptographic Controls
      a. All electronic Critical Information will be encrypted when in motion or at rest.
      b. All cryptographic keys will be protected against 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 McAfee security products.

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. If an Information System requires initial setup and configuration, this must be done without the Information System having direct access to the Internet. Only after all stable release updates and current security related patches are installed may an Information System be given direct Internet access.
4. Users must not accept any form of assistance or software to improve the security of their computers without approval by the Information Technology Services department.