POLICIES AND PROCEDURES

Information Technology Services

Asset Management

ISUPP 2430

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Asset Management*
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 identify, classify, and protect ISU's IT System.

II. DEFINITIONS

A. **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.

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

C. **Information Network:** A telecommunications network that allows Information Systems to electronically exchange data.

D. **Information Owner:** The ISU faculty, staff, or department responsible for accuracy, integrity, and timeliness of a defined subset of ISU's Information, and authorized to grant or deny access to that Information.

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. **Information System Administrator:** The ISU employee that is responsible for the protection and proper use of a specific Information System as assigned by an Information Owner.

H. **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.

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

J. **Public Information:** Information made freely available to the public or if disclosed is not expected to cause any harm to ISU or any individual associated with or accessing the information.

K. **Storage Media:** Devices designed and dedicated to storing data electronically (e.g., hard disk drives, tape drives and magnetic tape, flash drives, recordable CD/DVD, etc.)

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

III. POLICY STATEMENT

ISU has legal ownership of all Information stored, processed, or transmitted on its IT System, and reserves the right to access this information without prior notice whenever there is a genuine business need. ISU Information or Information entrusted to ISU from Third Parties will be classified based on its value, legal requirements, sensitivity, and criticality to the organization. Individuals creating, maintaining, using, or disseminating information must take reasonable precautions to protect it based on its assigned classification.

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 procedures are followed and for taking corrective action when Information and/or the IT System is or may be compromised.

V. PROCEDURES TO IMPLEMENT

A. Responsibility for Assets

1. Individual administrative and academic units will maintain a list of Information Systems and Information Networks for which they are directly responsible; a copy of this information will be provided to the Information Security Manager (see attachment: Information System Inventory Standard).
2. Individual administrative and academic units will assign an Information System Administrator to all Information Systems or Information Networks for which they are directly responsible.
3. Information System Administrators, working with the appropriate Information Owners, will classify the information stored, processed, or transmitted by Information Systems and Information Networks for which they are responsible, based on the information classification below, and will ensure that all relevant ISU information security policies are appropriately implemented.
4. Individuals creating, maintaining, using, or disseminating Critical Information or Institutional Information must take reasonable precautions to protect it from loss, misuse, unauthorized access or disclosure, and unintended alteration or destruction.

B. Information Classification

1. All ISU Information or information entrusted to ISU from Third Parties will be classified in one of the following three (3) categories:
    a. Critical Information: information identified by applicable laws, regulations or policies as restricted personally identifiable information, or sensitive scientific or sponsored project information. Access to this information will be tightly restricted based on legal requirements and the concept of “need to know”. Disclosure to external parties requires the existence of a signed confidentiality agreement (or equivalent) and the Information Owner’s documented approval, either in a signed

document or implicitly as part of a documented, organized authorization procedure. Critical information currently includes (but is not limited to):

i. Health information protected by HIPAA.

ii. The first name or first initial and last name of an individual, in combination with and linked to any one or more of the following data elements about the individual:

1. Social security number;
2. Driver's license number or state identification card number issued in lieu of a driver's license number;
3. Passport number;
4. Financial account number, credit card or debit card number, or financial account access codes;
5. Credit Card and other electronic commerce information protected by the Payment Card Industry Security Standards Council;
6. Government Export Controlled information.

b. Institutional: 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. Disclosure to an external party requires the Information Owner's verbal or written approval, based on the judgment of the Information Owner regarding the external party's trustworthiness, ability to properly protect the information, and existence of confidentiality agreements. Institutional information currently includes (but is not limited to):

i. Student record information protected by FERPA.

ii. Health records maintained in student files, i.e., immunization history, that are provided by the student for educational purposes are not considered HIPAA protected information. Such information becomes part of a student record and is covered by FERPA.

iii. Health information not covered by HIPAA.

c. Public: Information made freely available to the public or if disclosed, is not expected to cause any harm to ISU or any individual associated with or accessing the information. Access to this Information is freely available. Conversion to this

classification from a more sensitive classification level requires the Information Owner's approval.

2. If no classification has been assigned, information will be handled as though it is institutional.
3. If Information of various classifications is combined, the resulting collection of Information will be classified at the most sensitive level of the information contained in the collection.
4. Upon classification, the Information will be labeled and handled according to the Information Labeling and Handling Standard (see attachment).
5. The Information System will be classified identically to the classification of the most sensitive Information stored, processed, or transmitted by the Information System.
6. Upon classification, the Information System will be protected as outlined in the ISU information security policies.

C. Permission to Store Critical Information

1. Critical Information must not be stored on non-Information Technology Service-managed electronic devices or electronic media unless the following three (3) conditions have been met:
    a. A written justification is submitted to the Dean, Department Chair, or Vice President detailing why having Critical Information stored locally is absolutely necessary to conduct the business of the University and to perform the official duties of the person making the request.
    b. The Dean, Department Chair, or Vice President must grant written permission to the requesting individual, with a copy being sent to the departmental System Administrator and to Information Technology Services. While permission is not required to retain student grades, letters of recommendation, patentable research findings, etc., that are used regularly in the performance of faculty and staff duties, individuals storing such information on local devices must comply with ISU's information security policies in relation to this information.
    c. The individual must abide by ISU's information security policies in relation to the handling of all Critical Information which they have been granted permission to store locally on non-Information Technology Services-managed electronic devices or electronic media.
2. Critical Information transferred electronically, other than via fax or non-digital phone, must be conveyed using an encrypted method that meets current industry accepted standards for secure encryption. When sending Critical Information by fax it must be

clearly marked as confidential with an appropriate cover sheet. Reasonable effort should be made to ensure that only the intended recipient has access to the faxed information.

D. Permission to Store Institutional Information

1. Institutional information must not be stored on non-ISU owned hardware nor in cloud services that have not been approved by Information Technology Services.

VI. ATTACHMENT

Asset Management Standards

Attachment – Asset Management Standards

A. Information System Inventory Standard:

1. All Information Systems will be listed in an Information System Inventory Log maintained by the Information Security Manager that includes a record of the system name, owner, administrator, location, and classification.
2. System types may be one of the following:
    a. An individual Information System such as:
        - Desktop
        - Laptop
        - Server
        - Tablet
        - Mobile phone
        - Storage media
        - Networking device
    b. An Information System class, wherein the Information System is effectively duplicated in large numbers with only negligible variance in the security controls currently applied to the Information Systems (e.g., Administrative Workstations).
    c. Other asset types not listed above, as needed.

B. Information Labeling and Handling Standard:

1. Public and institutional classified information do not need explicit labeling nor are they subject to specific handling instructions.
2. Critical Information classified information will labeled as follows:
    a. Critical Information that may be electronically transmitted, printed, presented or stored on a general-purpose storage system will be labeled as “Critical Information” in the electronic file.
    b. Critical Information being saved to systems that are established exclusively for storing Critical Information do not need additional classification labeling.
    c. External Storage Media that contain Critical Information will be labeled with “Critical Information” on the exterior of the media.
3. Waste copies of Critical Information in printed form will be shredded before disposal.

4. Staff providing physical delivery of Critical Information will receive written confirmation of receipt before leaving the information.

C. Cloud Storage Standard:

1. BOX is the approved storage solution for ISU Information that needs to be stored in the Cloud unless an alternative has been approved by Information Technology Services.