POLICIES AND PROCEDURES

Information Technology Services

Asset Management and Information Classification

ISUPP 2430

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Asset Management and Information Classification*
Responsible Executive (RE): *Chief Information Officer*
Sponsoring Organization (SO): *Information Technology Services*
Dates: Effective Date: *March 28, 2016; TBD*
Revised: *May 4, 2018; May 2026*
Review Date: *May 2031*

I. INTRODUCTION

Idaho State University is responsible for the prudent stewardship of University-owned assets, including equipment, materials, property, and other tangible resources acquired to support its academic, research, clinical, and administrative operations. Effective asset management ensures accurate inventory records, promotes accountability, supports regulatory and financial reporting requirements, and protects University resources from loss, misuse, or improper disposition. This policy establishes the principles and expectations governing the acquisition, tracking, use, maintenance, and disposal of University Information Technology assets throughout their lifecycle.

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, protected health information, education

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

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

E. Information Network. A telecommunications network that allows Information Systems to electronically exchange data.

F. 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.

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

H. 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.

I. 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.

J. 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.

K. 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.

L. 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.)

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

N. Users. All members of the ISU community, including faculty, staff, volunteers, contractors, and visitors.

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 as needed to maintain normal business operations. 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. Idaho State University requires that

all University-owned assets be recorded, safeguarded, tracked, and maintained in accordance with established asset management policies and applicable state and federal regulations. University departments and employees are responsible for ensuring that assets under their control are used solely for authorized University purposes, are properly inventoried, and are promptly reported when transferred, missing, damaged, or disposed of. All acquisitions, movements, and dispositions of assets must follow approved University processes. This policy applies to all tangible University property regardless of funding source, location, or custodian.

IV. AUTHORITY AND RESPONSIBILITIES

A. Administrative or Academic Units. Assign an Information System Administrator to all Information Systems or Information Networks for which they are directly responsible. Updating and submitting annual inventories.

B. Chief Information Officer. 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. 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 System Administrators. Information System Administrators, working with the appropriate Information Owners, 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.

E. Information Technology Services. Charged with ensuring all procedures are followed and for taking corrective action when Information and/or the IT System is or may be compromised.

F. Users. Responsible for protecting Information and the IT System. 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.

G. Service Desk Manager. Responsible for asset management and set-up of University systems. The Service Desk Manager has the authority and responsibility to escalate issues of non-compliance to the CISO where needed.

V. PROCEDURES TO IMPLEMENT

A. Information System Inventory Standard

1. All Information Systems will be listed in an Information System Inventory Log maintained by the Chief Information Security Officer 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
        i. Desktop;
        ii. Laptop;
        iii. Server;
        iv. Tablet;
        v. Mobile phone;
        vi. Storage media; and,
        vii. 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 Classification.

1. All ISU Information or information entrusted to ISU from Third Parties will be classified in one of the following four (4) categories:
    a. Critical Information.
        i. Critical Information is information used for the purpose of conducting University business. The disclosure, alteration, or destruction of Critical Information could result in a high level of risk to the University. Critical Information includes information identified by applicable laws, regulations or policies as restricted Personally Identifiable Information (PII) or sensitive scientific or sponsored project information.
        ii. Access to Critical Information will be tightly restricted based on legal requirements and shared only on a need to know basis.
        iii. Disclosure of Critical Information to external parties requires authorization and the Information Owner's documented approval.

iv. Critical Information currently includes, but is not limited to:

1. Protected Health Information (PHI) as defined under HIPAA.
2. Health related information including any information concerning an individual's physical or mental health, medical condition, treatment, diagnosis or care whether or not it qualifies as PHI under HIPAA that is maintained at a University Health Care Clinic.
3. 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:
    a. Social security number;
    b. Driver's license number or state identification card number issued in lieu of a driver's license number;
    c. Passport number;
    d. Financial account number, credit card or debit card number, or financial account access codes;
    e. Credit Card and other electronic commerce information protected by the Payment Card Industry Security Standards Council; and,
    f. Government Export Controlled information.

b. Institutional.

i. Institutional Information is 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.

ii. Information that is not explicitly classified as Critical Information or Public Information should be treated as Institutional Information.

iii. 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.

iv. Institutional Information currently includes (but is not limited to):

1. Student record information protected by FERPA.
2. 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.

3. Health information not covered by HIPAA.

v. If no classification has been assigned, information will be handled as though it is Institutional Information.

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

c. Public.

i. Public Information is 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.

ii. Access to Public Information is freely available. Conversion to this classification from a more sensitive classification level requires the Information Owner's approval.

d. Combined Information.

i. 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.

ii. The Information System will be classified identically to the classification of the most sensitive Information stored, processed, or transmitted by the Information System.

C. Labeling and Handling

1. Upon classification, the Information will be labeled and handled as outlined in ISU Information Security procedures.

2. Permission to Store Critical Information. 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.

i. 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.

ii. 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.

3. 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.

4. Any user who becomes aware of suspected or actual mishandling of Critical Information must immediately report it to the CISO.

5. Information classified as Public and Institutional do not need explicit labeling nor are they subject to specific handling instructions.

D. Inventory and Reporting.

1. Individual Administrative and Academic Units must maintain a list of Information Systems and Information Networks for which they are directly responsible. This list must be provided to the Chief Information Security Officer on an annual basis.

2. Updated inventories must be submitted to the Chief Information Security Officer annually by October 31st of each year.

3. Computers or tablets which are six (6) years old or older and not in use shall be sent to surplus and the inventory system updated.

VI. RELATED LAWS AND POLICIES

A. ISUPP 2400 *Information Technology Service Acceptable Use*

B. ISUPP 2430 *Information Technology Services Asset Management*

C. ISUPP 2470 *Information Technology Services Electronic Messaging*

D. ISUPP 2520 *Information Technology Services Risk Management*