POLICIES AND PROCEDURES

Information Technology Services

Information Security

ISUPP 12130

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Information Security*
Responsible Executive (RE): *Chief Information Officer*
Sponsoring Organization (SO): *Information Technology Services*
Dates: Effective Date: *March 28, 2016 (5-4-18)*
Revised: *May 4, 2018*
Review Date: *May 2021*

I. INTRODUCTION

It is the objective of Idaho State University (ISU) to implement information security based on policies, procedures and standards that are established to ensure proper implementation, oversight, and management.

II. DEFINITIONS

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

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

C. **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.

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

E. **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).

F. **Office of General Counsel:** The administrative unit that handles legal counsel, pre-litigation, legal risk management, contract development, and compliance reviews.

G. **Workforce or Workforce Member:** Faculty, staff, contractors, and volunteers at ISU. Excludes students, unless they are performing a specific work function similar to faculty or staff.

III. POLICY STATEMENT

ISU Information must be consistently protected in a manner commensurate with its sensitivity, value, and criticality. ISU will implement and maintain written information security policies, procedures, and standards which establish requirements regarding handling, accessing, and using ISU's information resources regardless of the media on which information is stored, the locations where the information is stored, the technology used to process the information, or the people who handle the information.

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 is properly protected, and maintain policies, procedures, and standards that are appropriate for ISU.

V. PROCEDURES TO IMPLEMENT

A. Responsible Parties

1. Information Technology Services will provide centralized guidance, direction, authority, coordination, and enforcement for all information security activities.
2. Information Technology Services may review the configuration, programming, operation, maintenance, documentation, and training of any component of ISU's IT System to determine compliance with the information security policies.
3. Information Technology Services will establish procedures and processes as needed to ensure proper implementation of the information security policies.

4. The Chief Information Officer may require that they be allowed to review and approve agreements with third parties which can affect ISU's IT System before the agreements are finalized.
5. Policies and procedures established and maintained by Information Technology Services may not be the only information security polices applicable to ISU business units, academic units, facilities, and Workforce Members. Workforce Members are expected to be aware of and comply with additional policies and procedures covering areas such as HIPAA, FERPA, Research, etc. as applicable.

B. Development and Publishing

1. Information security policies applicable to the entire University community will be created and maintained by the Information Technology Services department.
2. Individual administrative or academic units may also create additional security policies and/or procedures specific to their area of responsibility (for example: HIPAA, FERPA, Research and Export Controls, etc.). Such policies and/or procedures shall not conflict with, reduce, or weaken the security protections established by the ISU information security policies.

C. Review and Modification

1. The Information Security Manager will review the information security policies whenever significant changes in the environment occur or when a security incident suggests review, and will record the results of the review process and any suggested modifications.

D. Exceptions

1. Exceptions to information security policies are permissible only in those instances where a risk assessment examining the implications of being out of compliance has been performed, and where a standard risk acceptance form has been prepared by the Information Owner or his/her delegate and approved in writing by the Chief Information Officer or his/her delegate (see attachment: Security Exemption Request Form).
2. The Information Security Manager will record all exceptions to the information security policies.
3. All exceptions to the information security policies will be reviewed at least annually by the Information Security Manager and will be amended or revoked as necessary.

E. Non-enforcement

1. The Information Security Manager's non-enforcement of any specific information security policy does not constitute an implied exception.

VI. ATTACHMENT

Security Exemption Request Form

Attachment – Security Exemption Request Form

Regarding policy or procedure number: ***example: ISUPP ####***

Dealing with the topic of: ***example: Critical security patches***

> I understand that compliance with ISU information security policies is expected for all administrative and academic units, departments, and information and communication systems. I have read the above-named policy or procedure and I believe that the control(s) described therein should not be required for the following: **Department:** ***example: ITS*** ***System(s): example: XYZ*** ***Server***

I furthermore understand that a control deficiency in one information system can jeopardize other information systems because erroneous data may be inherited, or because a conduit for an intruder to enter ISU systems may be created. I also understand that non-compliance in this instance may adversely affect the morale or willingness of staff to comply with information security policies, procedures, and standards.

I understand that an exception to information security policies, procedures, and standards is appropriate only when it would: (a) adversely affect the accomplishment of ISU business, and/or (b) cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance.

I have attached a written assessment of the risks associated with being out of compliance with the above-mentioned policy or procedure. This assessment answers the following questions:

What could happen? (threats/vulnerabilities)

…to the information in this system?

…to information on other systems sharing the same physical network?

How bad would it be? (impact)

How often might it occur? (frequency/probability)

How certain are the answers to the questions above? (uncertainty)

In assessing the potential impact should a major loss take place because this out-of-compliance situation existed, I have carefully evaluated the type and value of information that could be exposed to a breach (on the exempted systems as well as other systems to which the exempted system could serve as a conduit).

Based on the Overall Risk chart below, I rate the impact and likelihood as follows:

Impact (1—3): Likelihood (1—3):

Impact	Disastrous (3)	**Low**	**High**	**Critical**
	Moderate (2)	**Low**	**Medium**	**High**
	Insignificant (1)	**Low**	**Low**	**Low**
		Rare (1)	Moderate (2)	Likely (3)
	Likelihood			

Based on this assessment, I judge the risk to ISU to be 'LOW' and I request that an exemption be approved. I understand that, if granted, this exception will expire one (1) year from the date of approval.

Signature of responsible manager

Signature of the CIO

Printed name of responsible manager

Printed Name of the CIO

Date signed

Date signed

This risk assessment has been reviewed and approved by the ISU's Chief Information Officer.