POLICIES AND PROCEDURES

Information Technology Services

Risk Management

ISUPP 2520

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Risk 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 establish a holistic, consistent, and systematic approach to managing Information security risk.

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

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

E. **Information Owner:** The ISU employee 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.

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

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. **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. **Risk Assessment:** A repeatable process for determining Information security risk.

III. POLICY STATEMENT

ISU will manage Information security risk for its IT System by performing Risk Assessments and then treating the discovered risks in a reasonable manner.

IV. AUTHORITY AND RESPONSIBILITIES

All members of the ISU community, including faculty, staff, volunteers, contractors, and visitors are responsible to abide by acceptable access procedures as outlined in this policy.

The Information Technology Services department is charged with seeing that all procedures are followed and for taking corrective action when access to Information and/or the IT System is or may be compromised.

V. PROCEDURES TO IMPLEMENT

A. Risk Assessment

1. Each individual ISU administrative and academic unit which manages its own Information Systems or Information Networks will assign an Information System Administrator to help manage those systems and networks (see *Information Technology Services Asset Management ISUPP 2430*.

2. Information System Administrators will be responsible for performing a security-related Risk Assessment of the organizational unit's Information resources following the standards outlined in the attached Risk Assessment Standards.
3. Once the security-related Risk Assessment is complete, the appointed Information System Administrator will provide the Information Security Manager with a copy of the documentation resulting from the Risk Assessment as well as a signed letter certifying that adequate security measures have been implemented.
4. The Risk Assessment will be performed before the Information System or Information Network is allowed to connect to ISU's current infrastructure, and annually thereafter or whenever there is any significant change in the environment.

B. Risk treatment

1. A risk remediation plan will be created listing all "Critical", "High", and "Medium" risks discovered and the selected Risk Treatment Standard (see Attachment—Risk Management Standards) for each risk.
2. Low risks do not need to be listed in the risk remediation plan.
3. The Information Security Manager will approve all risk remediation plans.

C. Remediation Plan implementation

1. All risks will be treated according to the Risk Treatment Standard.
2. The Chief Information Officer will approve risk acceptance of all "Critical" or "High" risks.
3. The Information Security Manager will approve risk acceptance of all "Medium" risks.
4. Low risks are implicitly accepted by ISU.

VI. ATTACHMENT

Risk Management Standards

Attachment – Risk Management Standards

A. Risk Assessment Standard:

1. All Information Systems and Information Networks will be identified and documented according to the Information System Inventory Standard (see Information Technology Services Asset Management ISUPP 2430).
2. All security controls currently applied to the individual Information Systems and Information Networks will be documented.
3. For each Information System and Information Network, current threats and vulnerabilities will be documented.
4. For each threat and vulnerability combination, the likelihood that the threat will exploit the vulnerability will be estimated and documented as follows:
    - Rare: may happen once ever ten (10) or more years.
    - Moderate: may happen once every five (5) years.
    - Likely: may happen annually or more frequently.
5. For each threat and vulnerability combination, the impact caused by the threat exploiting the vulnerability will be estimated and documented as follows:
    - Insignificant: other security controls would have to fail for the threat to fully exploit the vulnerability OR multi-minute or no interruption of operations OR no breach of data occurred.
    - Moderate: creation of a new vulnerability OR multi-hour interruption of operations OR breach of institutional data OR minor breach of Critical Information data occurred.
    - Disastrous: creation of multiple new serious vulnerabilities OR multi-day interruption of operations OR major breach of Critical Information.
6. For each threat and vulnerability combination, the risk will be calculated and documented using the estimated Likelihood and Impact according to the following matrix:

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

B. Risk Treatment Standard:

1. For each Critical, High, or Medium Risk discovered, the risk to the Information System and Information Network will be reduced by one of the following methods:

    - Risk Avoidance – The Information System, Information Network (or a component thereof) will be decommissioned.
    - Risk Transfer – The Information System, Information Network (or a component thereof) will be outsourced.
    - Risk Mitigation – New security controls will be implemented to further protect the Information System or Information Network.
    - Risk Acceptance – The risk will be accepted and no changes will occur in the environment.