POLICIES AND PROCEDURES

Information Technology Services

Compliance and Sanctions

ISUPP 12090

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Compliance and Sanctions*
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

The greatest threat to privacy and security rests within an organization's workforce. In an attempt to hold organizations accountable, federal and state laws have mandated breach prevention and penalties, which are becoming more stringent. It is the objective of Idaho State University (ISU or University) to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The University must be prepared to respond fairly and appropriately (1) to violations of law, regulation, or University policy relating to information security, (2) when questionable or unacceptable computing practices occur, or (3) where there is noncompliance with information security policy requirements or with reasonable requests for action or cooperation necessary to implement the University's information security policies.

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 *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.

J. **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 requires that faculty, staff, students, volunteers, and contractors comply with all applicable laws, regulations, statutes, and University policies relating to information security and information technology. Lack of compliance will result in sanctions or other appropriate action which are consistent and relevant not only to the incident but to the potential for harm.

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 auditing the use of ISU IT systems by all faculty, staff, students, volunteers, contractors, and visitors to ensure the security of all ISU Information through compliance with University policies.

V. PROCEDURES TO IMPLEMENT

A. Compliance with Legal Requirements

All Information Systems containing Critical Information will be compliant with applicable government laws and industry regulations and ISU policies and Procedures.

B. Compliance with Security Policies, Standards, and Technical Compliance

1. Managers of all administrative and academic units will ensure compliance with ISU Information Security Policies within their areas of responsibility by performing regular review of compliance and promoting awareness amongst faculty, staff, and student employees.
2. The Information Security Manager will periodically review compliance with ISU information security policies across all organizations within ISU through onsite interviews, inspections, and audits.
3. All Workforce Members are required to report any actual or suspected violation of the ISU information security policies. The report is to be made to the Information Security Manager via an email sent to security@isu.edu.
4. Violations of ISU information security policies will be recorded, monitored, and updated (as remediation occurs) by the Information Security Manager.

C. Sanctions

1. Sanctions for privacy and information security-related violations shall be applied consistently irrespective of the status of the violator, with comparable discipline imposed for comparable violations.

VI. ATTACHMENT

Compliance and Sanctions Standards

Attachment – Compliance and Sanctions Standards

A. Sanctions Standard:

1. The Chief Information Officer shall be responsible for determining whether a violation has occurred. Human Resources (for faculty or staff) or Student Affairs (for students) will be responsible, in consultation with the Chief Information Officer and the Chief Compliance Officer, to determine what sanctions should be imposed.
2. ISU defines categories that establish the significance and impact of the privacy or security incident to help guide corrective action and remediation.
    a. Category 1: Unintentional breach of security that may be caused by carelessness, lack of knowledge, or lack of judgment, such as an error that causes a billing statement to be mailed to the wrong individual or organization.
    b. Category 2: Deliberate unauthorized access to confidential or sensitive information without disclosure. Examples: snoopers accessing confidential information without legitimate business reason, password sharing, or other failure to follow policy without legitimate reason.
    c. Category 3: Deliberate unauthorized disclosure of or tampering with confidential or sensitive information without malice or personal gain. Examples: sharing unauthorized confidential or sensitive information with the news media, unauthorized modification of an electronic document to expedite a process.
    d. Category 4: Deliberate unauthorized disclosure of or tampering with confidential or sensitive information for malice or personal gain. Examples: identity theft, or selling of confidential or sensitive information.
3. Factors that may modify application of sanctions:
    a. Sanctions may be modified based on mitigating factors.
        - Multiple offenses
    b. Factors that could mitigate sanctioning could include:
        - Offender voluntarily admitted the breach and cooperated with the investigation.
        - Offender was inadequately trained or not aware of policy.
    c. Possible Sanctions could range from a verbal warning to suspension and/or dismissal.