POLICIES AND PROCEDURES

Information Technology Services

Communications and Operations Management

ISUPP 2450

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Communications and Operations 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 operate stable and secure information processing facilities.

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. **Essential Computing Resources:** Shared computing resources which cannot undergo loss of access for more than twenty-four (24) hours without causing unacceptable consequences due to a break in business continuity.

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

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

H. **Information System:** A computing device that stores, processes, or transmits ISU Information.

I. **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.

J. **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.

K. **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.

L. **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.

M. **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.).

N. **Virtual Private Network (VPN):** Software that extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

III. POLICY STATEMENT

ISU will manage key areas in day-to-day information operations to help ensure that its Information is available and protected against data corruption, loss, or misuse.

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 making sure that Information is available as needed and properly protected.

V. PROCEDURES TO IMPLEMENT

A. Operational Procedures and Responsibilities

1. A list of applications, their owners, and functions will be maintained for all Essential Computing Resources.
2. Standard operating procedures will be maintained for all Essential Computing Resources.
3. Operational duties will be segregated for Essential Computing Resources, whenever possible.
4. Changes to Essential Computing Resources will be assessed for potential negative impact and approved by at least two (2) individuals prior to implementation.
5. Separate development and production Information Systems will be used for Essential Computing Resources, wherever possible.

B. Third-party Service Delivery Management

1. Third party service providers will be monitored by the purchasing entity to ensure compliance with the ISU information security policies and service level agreements.
2. Internet domain names must only be registered with a registrar that provides a sufficient level of security and an acceptable change control procedure, as determined by the Information Security Manager.

C. System Planning and Acceptance

1. The use of ISU IT System resources will be monitored and tuned by the responsible Information System Administrator to ensure that capacity requirements are met now and in the future.
2. Acceptance criteria for new Information Systems or changes to existing systems should be established and suitable tests carried out prior to acceptance.

D. Protection Against Malicious Code

1. All ISU Information Systems will be protected by anti-malware software centrally managed by Information Technology Services.
2. Reports on the update status of all anti-malware client software will be reviewed weekly and Information Systems that are not regularly updating will be investigated and repaired.
3. All vendor supplied critical security patches applicable to ISU Information Systems will be installed within thirty (30) days of their release.
4. The security of an ISU Information System must never be entirely dependent on the security of another computer system.

E. Data Backup

1. Data backup solutions will adhere to established business continuity policies (see *Information Technology Services Business Continuity Management* ISUPP 2440).

F. Network Security Management

1. Essential Computing Resources will be redundant, whenever possible.
2. Essential Computing Resources will log relevant security actions and activity will be reviewed regularly for notable security events.

G. Media Handling

1. Any Storage Media containing Institutional Information or Critical Information will be appropriately erased prior to re-use.
    a. Media Erasure Standard
        i. Traditional magnetic disk media will be sanitized via a minimum one-pass, pseudo-random overwrite of the entire media storage space.
        ii. Solid-state drives (SSD) will be sanitized using the “ATA Secure Erase” method of erasure.
        iii. If these options are not viable, the responsible Information System Administrator will work directly with Information Technology Service’s information security department to identify and implement an acceptable erasure option.
2. Re-use of Storage Media that contained Critical Information from entities outside of ISU is not permitted.
3. Any Storage Media containing Critical Information will be physically destroyed before disposal.

H. Exchange of Information

1. Contractual agreements will be established and approved by the Chief Information Officer for any exchange of data between ISU and third parties.
2. All information exchanged with third parties by way of physical Storage Media or electronic transfer will be encrypted using methods approved by the Information Security Manager (see also *Information Technology Services Access Control* ISUPP 2410).
3. The Information Security Manager will approve the enabling of access by external parties to internal Information System data sharing ports.
4. The Information Security Manager will approve establishment of VPN tunnels to/from third parties.

I. Electronic Commerce

1. All credit card processing at ISU will be outsourced to an external, certified, Payment Card Industry Data Security Standard (PCI DSS) compliant service provider as specified by the ISU Controller.
2. Any contractual agreement for outsourced credit card processing will be pre-approved by the Chief Information Officer and the ISU Controller.
3. Unencrypted protected credit card information will not reside on nor transfer through ISU's IT System.
4. Encrypted protected credit card information must be encrypted before it reaches ISU's IT System.
5. Encrypted protected credit card information must be encrypted in such a manner that only the outsourced credit card processing service provider can decrypt the information.
6. Encrypted protected credit card information may only be staged while in transit to an external credit card processing service provider.
7. ISU controlled, public facing web applications that collect credit card payments will integrate with an external service provider in such a way that protected credit card information is never retained on ISU owned or controlled storage.

J. Monitoring

1. ISU Information System Administrators may monitor network usage on the ISU Information System for which they are responsible and keep appropriate records.
2. ISU Information System Administrators may regulate bandwidth utilization.

3. Information System Administrators for all Information Systems containing Critical Information and all Essential Computing Resources will generate audit logs, whenever possible, and protect against tampering with or unauthorized access of these logs.
4. Audit logs will contain, at a minimum:
    a. User session activity including user IDs, logon date and time, logoff date and time,
    b. Application activity including applications invoked,
    c. Changes to critical application system files,
    d. Changes to the privileges of users,
    e. System start-ups and shut-downs.
5. Audit logs will automatically copy to an essential audit log storage system on a daily basis.
6. Audit logs containing security relevant events must be retained for at least three (3) months, during which time they must be secured such that they cannot be modified, and such that only authorized persons can read them.
7. Audit log reports will be reviewed at least once a week and unexpected events will be investigated. This process will be automated to produce reports on critical operation and security events whenever feasible.