POLICIES AND PROCEDURES

Information Technology Services

Physical and Environmental Security

ISUPP 12140

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Physical and Environmental Security*
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 provide reasonable physical and environmental protections for its Information and IT System.

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 as defined in the *Information Technology Services Asset Management ISUPP 2430*.

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

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

G. **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.

H. **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.).

III. POLICY STATEMENT

ISU will implement reasonable physical and environmental controls (appropriate to the identified risks and the value of the assets protected) that attempt to prevent unauthorized physical access, interference, or physical damage to its IT System resources.

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 proper controls are in place to protect ISU's Information and/or the IT System.

V. PROCEDURES TO IMPLEMENT

A. Secure Areas

1. Information Systems with Critical Information will be physically secured in such a manner as to deter (as determined by the Information Security Manager) unintended physical access or damage.
2. Information Systems that contain Critical Information will not be taken off-premise without the Critical Information being encrypted by disk or file encryption approved by the Information Security Manager.

3. Information Systems containing Critical Information will be positioned in such a manner as to minimize viewing from unauthorized individuals.
4. Outside of regular working hours, unless they are working at the time, all faculty, staff, and student employees will clean their desks and working areas such that all sensitive or valuable data is properly secured.
5. Rooms containing Essential Computing Resources will implement the following additional protections:
    a. Essential Computing Resources will not be located on non-ISU property without written approval from the Chief Information Officer.
    b. Entrances will not advertise the room's purpose.
    c. Entrances will be monitored by a video surveillance system and/or an unauthorized entry notification system.
    d. Essential Computing Resources will be secured in protective enclosures.
    e. Access for maintenance and configuration purposes will be kept to an absolute minimum.
    f. Windows will be avoided or, if not avoidable, will be barred for prevention of entry.
    g. Faculty, staff, and student employees will record the date and time of entry and exit.
    h. Visitors will be escorted at all times by an appropriate faculty, staff, or student employee and the date and time of entry and exit will be recorded.

B. Environmental Controls
1. Cables carrying power or data to Essential Computing Resources or Information Systems with Critical Information will be protected by one or more of the following:
    - placement underground,
    - placement in ceilings,
    - placement in cabling conduit, or
    - contained within a locked room
2. For Essential Computing Resources, the following additional environmental controls will be observed:
    a. Substances such as food or drink will not be taken into rooms containing Essential Computing Resources.

b. Essential Computing Resources will be protected with uninterruptable power supplies and, if reasonable, by a power generator.

c. Essential Computing Resources will be protected with appropriate heating, ventilation, and air conditioning to maintain proper operating temperatures and humidity for the environment.

d. Rooms containing Essential Computing Resources will be protected with fire protection/suppression systems. Fire protection/suppression systems that do not contain water will be used whenever possible.

e. Essential Computing Resources will be protected by a manufacturer warranty or redundant systems, whenever possible.

f. Mobile Storage Media from Essential Computing Resources will be stored in appropriately designed fire and waterproof safes.