POLICIES AND PROCEDURES

Information Technology Services

Security Roles and Responsibilities

ISUPP 12110

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Security Roles and Responsibilities*
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 ensure that Workforce Members utilizing ISU's IT System do so in a secure manner.

II. DEFINITIONS

A. **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.

B. **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.

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

D. **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.

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. **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

Security roles and responsibilities of employees, contractors, and third-party users will be defined and documented in accordance with ISU's information security objectives.

IV. AUTHORITY AND RESPONSIBILITIES

All Workforce Members are responsible for protecting Information and the IT System.

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

V. PROCEDURES TO IMPLEMENT

A. Prior to employment

1. Specific information related to security responsibilities will be articulated in job descriptions for Workforce Members that will have access to Critical Information or Institutional Information.
2. Workforce members are required to annually agree to ISU's acceptable use agreement prior to being granted continued access to ISU's IT System (see Information Technology Services Acceptable Use ISUPP 2400).

B. During Employment

1. All Workforce Members must take reasonable precautions to avoid exposing Critical Information in public places such as in building lobbies, airplanes, restaurants, elevators, public transportation, etc.
2. Unofficial comments that Workforce Members post to an electronic mail system, an electronic bulletin board system, or other electronic systems must not be represented as though they are formal statements of, or the official position of, ISU.
3. Training
    a. The Information Security department within Information Technology Services will arrange for Workforce Members to be trained on the basics of information security (including the identification, response, and reporting of information security events or weaknesses) and a record will be kept of their completion of the training. Information Security will also make Workforce Members aware of urgent information security threats in a timely manner.
    b. Job training for all Workforce Members in computer-related positions of trust will include training on ISU information security policies. The department, as part of its normal job training, will provide this training for new employees.
    c. All Workforce Members will be made aware that ISU's IT System is monitored and that causing an information security incident will be appropriately disciplined, up to and including termination (see Information Technology Services Compliance and Sanctions ISUPP 2460).

C. Termination or Change of Employment
1. The individual administrative or academic unit, in conjunction with Human Resources, will be responsible for termination procedures for all Workforce Members. These procedures will include notification to the Information Technology Security Manager when termination is imminent.
2. The individual administrative or academic unit will ensure that keys or other physical access devices are returned within a reasonable amount of time following notice of termination of the Workforce Member.
3. The individual administrative or academic unit will disable the Workforce Member's local operating system and application accounts within twentyfour (24) business hours of being notified of the termination of the Workforce Member with the exception of Google Apps accounts which will be disabled as explained in Information Technology Services Electronic Messaging ISUPP 2470.
4. Information Technology Service will disable the workforce member's access to any Essential Computing Resources within twenty-four (24) business hours of being notified of the termination of the Workforce Member.