**POLICIES AND PROCEDURES**

**Information Technology Services**

**Incident Management**

**ISUPP 12120**

*POLICY INFORMATION*
**Policy Section:** *Information Technology Services*
**Policy Title:** *Information Technology Services Incident Management*
**Responsible Executive (RE):** *Chief Information Officer*
**Sponsoring Organization (SO):** *Information Technology Services*
**Dates: Effective Date:** *March 28, 2016 (5-4-18)*
**Revised:** *September 18, 2018*
**Review Date:** *September 2021*

## I. INTRODUCTION

It is the objective of Idaho State University (ISU) to ensure information security events and weaknesses associated with Information Systems are communicated in a timely manner and that appropriate corrective action is taken.

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

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

E. **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.

F. **Office of General Counsel:** The administrative unit that handles legal counsel, pre-litigation, legal risk management, contract development, and compliance reviews.

## III. POLICY STATEMENT

ISU requires that security incidents be handled in a secure manner following a predefined course of action.

## 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 communicating any issues with Information Systems and correcting such issues.

## V. PROCEDURES

A. Reporting Incidents

1. Any known or suspected information security event or weakness will be reported to the manager of the administrative or academic unit immediately. Incidents that may involve the administrative or academic manager should be reported to the appropriate Vice President or the Chief Information Officer.
2. Managers of administrative or academic units that can't positively determine that the reported security event or weakness was a false positive will report the suspected information security event or weakness to the Chief Information Officer or the Information Security Manager immediately.

B. Managing Incidents

1. The Information Security Manager will lead all security incident response and recovery efforts and will follow a documented process to respond to reports of information security events or weaknesses.
2. The Chief Information Officer or Information Security Manager will immediately notify the ISU Office of General Counsel when reports of information security events or weaknesses involving Critical Information are confirmed to be true positives.
3. The Information Security Manager will ensure proper chain-of-custody of evidence when it is suspected that the information security event may result in legal action.
    a. Incident Management Standards
        i. Time Clocks
            1. To facilitate incident response, the internal clocks of all Information Systems storing, processing, or transmitting Critical Information or Institutional Information will be synchronized to a common time source.