Idaho State University

POLICIES AND PROCEDURES

Information Technology Services

Business Continuity Management

ISUPP 2440

POLICY INFORMATION
Policy Section: *Information Technology Services*
Policy Title: *Information Technology Services Business Continuity 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 counteract interruptions to business activities and to protect critical business processes from the effects of major failures of Information Systems or disasters and to ensure their timely resumption.

II. DEFINITIONS

A. **Business Continuity Plan (BCP):** A document containing information and action plans that a functional unit has determined would be needed to help ensure that business processes can continue during a time of emergency or disaster.

B. **Business Impact Analysis (BIA):** A process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on a functional unit's operations.

C. **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.

D. **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.

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. **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.

H. **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.

I. **Recovery Point Objective (RPO):** The maximum interval of time that a department pre-determines that it can allow to pass during a disruption before the quantity of data lost during that period would result in unacceptable business consequences.

J. **Recovery Time Objective (RTO):** The maximum amount of time that a department pre-determines that computers, systems, networks, or applications can be unavailable following a failure or disaster before the consequences of the interruption become unacceptable.

K. **Risk Assessment:** A repeatable process for determining information security risk (see Information Technology Services Risk Management ISUPP 2520).

L. **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 requires that events that can cause interruptions to business processes be identified and continuity plans created that detail recovery objectives and methods.

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 identifying critical processes and developing continuity plans to recover Information in the event of a system failure.

V. PROCEDURES TO IMPLEMENT

A. Information System Administrators will be responsible for performing the following information security aspects of business continuity management:

  1. A Risk Assessment documenting in writing all Information Systems that store or cache Critical Information or Institutional Information. This Risk Assessment will note if formal continuity plans should be created or if other security controls negate the need for a formal continuity plan. If other security controls negate the need for a formal continuity plan, these other controls must be enumerated in the written Risk Assessment;
  2. A Business Impact Analysis for any Information System for which it was determined that a formal continuity plan should be created;
  3. Preparation of a Business Continuity Plan for any Information System for which it was determined that a formal continuity plan should be created. This plan will contain at a minimum the following:
     a. Procedures detailing the decision-making authorities, points of contact, and authorization steps necessary to enable invocation of the Business Continuity Plan;

     b. Procedures that ensure facilities and information system security controls remain intact or are replaced with equivalent controls throughout execution of the Business Continuity Plan;

     c. Documented Recovery Point Objectives (RPOs) and a plan for data backup and recovery that details the procedures that will be implemented to meet the desired RPOs;

     d. Documented Recovery Time Objectives (RTOs) and a plan for data backup and recovery that details the procedures that will be implemented to meet the desired RTOs.
  4. Business Continuity Plans will be tested as needed and updates incorporated when appropriate.

VI. ATTACHMENT

Business Continuity Management Standards

Attachment – Business Continuity Management Standards

A. Business Impact Analysis Standard:

1. Recovery Point Objectives (RPOs) will be established which will:
    - be defined in minutes, hours, or days,
    - consider the end user impact (e.g., frustration, data recovery effort, etc.),
    - consider the reputational harm to ISU,
    - consider the cost to recreate the data,
    - consider the impact to the end user, Information Owner, and/or ISU if the data could never be recreated.
2. Recovery Time Objectives (RTOs) will be established which will:
    - be defined in minutes, hours, or days,
    - consider the temporary end user impact (e.g., frustration, data recovery effort, etc.) for an unavailable application,
    - consider the reputational harm to ISU,
    - consider the cost to restore the Information Systems to full operation,
    - consider the impact to the end user, Information Owner, and/or ISU while the Information System is unavailable.

B. Data Backup Standard

1. Data backups of Information Systems containing Critical Information or Institutional Information will occur at a frequency to meet or exceed the Recovery Point Objective (RPO).
2. Storage Media used for backup purposes, which contains Critical Information or Institutional Information, will be encrypted via an encryption algorithm approved by the Information Security Manager.
3. Backup copies of Critical Information or Institutional Information that will be stored with a third party will be encrypted with a private key known only to ISU.
4. Storage Media used for backup purposes, which contains Critical Information or Institutional Information, will be tested via random sampling as needed to provide a reasonable level of assurance that the contents of the Storage Media can be restored.
5. Storage Media used for backup purposes, which contains Critical Information or Institutional Information, will be stored in a separate, secure facility located in a separate

fire zone whenever possible, and a record will be maintained of the transfer of the Storage Media.

6. Storage Media used for backup purposes must be monitored and refreshed as needed to assure that sensitive, critical, or valuable information stored for prolonged periods of time is not lost due to media deterioration.
7. Storage Media used for backup purposes, which contains Critical Information or Institutional Information, will be retained according to any state or federal regulatory requirements.
8. Mobile Storage Media used for backup purposes, which contains Critical Information or Institutional Information, will be stored in media-grade locked cabinets or safes, and in locked rooms.