Idaho Technology Authority (ITA)

ENTERPRISE GUIDELINES – G100 GENERAL

Category: G115 – BUSINESS RECOVERY PLAN

CONTENTS:

I. DEFINITION

Business Recovery Planning - The documentation, plans, policies, and procedures that are used to restore normal operation to a State Agency impacted either by a natural disaster or a significant disruption to normal services. [ITA Policy P2020 (Business Recovery Planning)].

II. RATIONALE

These guidelines are intended to assist Agencies in the evaluation and preparation of Information Technology (IT) Business Recovery Plans. An Agency's IT Business Recovery Plan could be a separate program or it could be part of a larger Agency program (Agency Business Recovery Plan, Disaster Recovery Plan, Business Continuity Plan, Business Contingency Plan, etc.).

III. GUIDELINE

1. The following set of questions can be used as a guideline to evaluate an IT Business Recovery Plan:

   A. Does the plan address both IT and telecommunications services?

   B. Does the plan address the full range of natural or man-made events (to include acts of terrorism and the potential use of weapons of mass destruction) that could result in a disruption of IT services?

   C. Is the plan periodically (as defined in ITA Policy P2020 (Business Recovery Planning) reviewed and updated?

   D. Is the plan stored in multiple locations and/or data formats to ensure its availability regardless of where a contingency may occur?

E. Does the plan include procedures to notify key personnel?

F. Does the plan address information about staffing and responsibilities, to include detailed assignments that show what actions to take during a contingency?

G. Does the plan address training of recovery personnel in the testing and operation of the plan?

H. Does the plan identify a list of critical systems, data, applications, staff and equipment?

I. Does the plan prioritize the services to be restored?

J. Does the plan address steps taken to mitigate the impact of the contingency?

K. Does the plan include procedures to retrieve equipment, supplies, files and other materials from a damaged location?

L. Does the plan include procedures for attempting to recover lost data?

M. Does the plan include procedures for restoring and returning to the original operational condition after the event is over?

N. Has the plan been successfully tested to ensure the continued availability and integrity of Agency systems and data?

O. If alternate equipment and spares are not available to support Agency systems during an emergency, has a plan been established to rapidly acquire new equipment, if needed?

P. Does the criticality of Agency systems or data warrant the need for an alternate operations site in the event the primary site(s) is/are disrupted?

2. **If so, questions A. through D. below also apply:**

A. Have alternate operations sites been identified with compatible equipment and environmental requirements (e.g., telecommunications circuits, power, etc.)?

B. Have the alternate operations sites been successfully tested?

C. Are the alternate operations sites scheduled to be tested on a periodic basis?

D. Do the alternate operations sites provide the necessary physical security for Agency systems?

IV. PROCEDURE REFERENCE

Policies for business recovery plan are detailed in ITA Policy P2020 (Business Recovery Planning).

The following resources are available to assist Agencies with the evaluation and preparation of Business Recovery Plans:

1. The Idaho Bureau of Homeland Security
   http://www.bhs.idaho.gov

2. *The State of Idaho Safety and Loss Control Model* (Revised August 2001)
   http://adm.idaho.gov/risk/pdf/Safety_and_Loss_Model_2002.pdf

   Guidelines for Business Recovery Planning are contained in: Section 3.4 entitled "Emergency Management Program"

3. Federal Emergency Management Agency (FEMA) Publication:

   Emergency Management Guide for Business & Industry – A Step-By-Step Approach to Emergency Planning, Response and Recovery for Companies of All Sizes
   http://www.fema.gov/pdf/library/bizindst.pdf

4. National Institute of Standards and Technology (NIST) Special Publication SP 800-34 entitled *Contingency Planning Guide for Information Technology Systems*, dated June 2002.
   http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

For additional resources or more information, contact the ITA staff at (208) 332-1876.

V. CONTACT INFORMATION

For more information, contact the ITA Staff at (208) 605-4064.

REVISION HISTORY

07/01/13 – Changed "ITRMC" to "ITA".

6/16/09 – Added Procedure Reference, Contact Information and Revision History to this guideline; changed the layout and deleted Additional Resources and Timeline.

   Revised: December 11, 2002
   Effective Date: October 17, 2001