Business Continuity Management Program

Disaster Recovery Planning Policy

*Project ID: FSEP / E&Y BCM Audit Response*

Prepared by: W. Regensburger

**Project ID:** EY/BCP/DR Audit Response  
**Version:** 1.0  
**Version Date:** 02/1/16

**Confidentiality Notice**
The information contained in this document was prepared by the University of Southern California Fire Safety & Emergency Planning Office (FSEP). This document and the information contained in it are considered private and confidential to FSEP. No part of this document may be reproduced, reused, or distributed to other parties without the express consent of USC FSEP. If you are in possession of this document and you are not sure whether or not you should be, call the Fire Safety & Emergency Planning department at **(213) 740-6197** for information on how to return or dispose of the document.
1 DOCUMENT REVISION HISTORY

This section describes the changes that have been made to this document following its initial development.

<table>
<thead>
<tr>
<th>Date</th>
<th>Ver.</th>
<th>Description of Change</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/2/2016</td>
<td>1.00</td>
<td>Initial Draft</td>
<td>W. Regensburger</td>
</tr>
</tbody>
</table>

2 PROJECT CHANGE SUMMARY

This section describes the changes that have been made to this project following its initial acceptance by the stakeholders and approval for implementation.

<table>
<thead>
<tr>
<th>Date</th>
<th>Ver.</th>
<th>Description of Change</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

1. **DOCUMENT REVISION HISTORY** ........................................................................................................... 2  
2. **PROJECT CHANGE SUMMARY** ............................................................................................................ 2  
   1. **INTRODUCTION** .............................................................................................................................. 4 
      1.1 **PURPOSE** ................................................................................................................................ 4 
      1.2 **SCOPE** .................................................................................................................................... 4 
      1.3 **GOAL** ...................................................................................................................................... 4 
      1.4 **DOCUMENT MAINTENANCE** ....................................................................................................... 4  
   2. **KEY STAKEHOLDERS** ....................................................................................................................... 4 
      2.1 **COMMUNICATION RESPONSIBILITIES** ......................................................................................... 5 
   3. **DISASTER RECOVERY PLAN KEY ELEMENTS** .................................................................................. 6
1. **INTRODUCTION**

1.1 **Purpose**

This policy describes the key elements that should be included in a department or school IT Disaster Recovery Plan (DRP). (See also: Disaster Recovery Plan sample/template)

1.2 **Scope**

The DRP Policy outlines IT recovery goals and recovery expectations of all stakeholders. The policy will be used to provide guidance to the Business Continuity Management Project. Effective recovery of information and information systems following a disaster or disruption is critical to the university mission.

1.3 **Goal**

To ensure that all university Disaster Recovery Plans are effective, and consistent, providing complete documentation of information technology backup and restoration procedures, and maintain compliance with requirements and best practice standards.

1.4 **Document Maintenance**

This document will be reviewed annually and updated as needed, as the project proceeds through each phase of the Business Continuity Management Project life cycle.

This document contains a revision history log. When changes occur, the document’s revision history log will reflect an updated version number as well as the date, the owner making the change, and change description will be recorded in the revision history log of the document.

2. **KEY STAKEHOLDERS**

This section describes the roles and responsibilities of the Business Continuity Management stakeholders with regard to the Communication Plan. Listed below are the key stakeholders:

- Crisis Management Team
- BCM Steering Committee
- Executive business sponsor (Dave Wright)
- Program Administrator (FSEP)
- School/Department Coordinator (Team Planner)
- Program owner (Team Leader)
- IT Disaster Recovery Program Coordinator (School/Dept. IT Admin)
- USC Medical Enterprise Program Coordinator (Robert Vance)
- USC Medical Enterprise Program Owner (Paul Craig)
- USC Central ITS CIO (Doug Shook)
2.1 Communication Responsibilities

Crisis Management Team
- The team will communicate and provide direction through the Executive Business Sponsor.

BCM Steering Committee
- The BCP will provide recommendations about communications and serve as a liaison between the Program Administrators and Crisis Management Team.

Executive Business Sponsor
- Communicate BCM expectations and accountabilities relating to plan development, maintenance, training and testing of Business Continuity and Disaster Recovery plans.

Program Administrator
- Ensure the executive business sponsor is kept informed of the status of planning and other program components.
- Communicate the need to perform plan maintenance, training, and exercise to the recovery team planners and team leaders.
- Provide regular training to ensure that all stakeholders are aware of the BCM program and their responsibilities. See training policy document for details.
- Provide informational content for steering committee and crisis management team meetings.
- Stay apprised of and communicate BCM industry trends and best practices.

IT Disaster Recovery Program Coordinator
- Communicate with the Program Administrator and central Information Technology Services to ensure compliance with plan updates and testing.
- Communicate issues relating to recoverability of IT systems that do not align with business needs.

School/Department Program Owner & USC Medical Enterprise Program Owner
- Communicate with the recovery team planner and recovery team members to ensure program compliance, expectations and accountabilities for business continuity and disaster recovery deliverables, including BIA, plan development and maintenance, testing and training.

School/Department Program Coordinator & USC Medical Enterprise Program Coordinator
- Communicate with recovery teams and the team leader to ensure key deadlines are met. Other communications will include the scheduling of meetings, training and exercises.
- Communicate plan development, maintenance and status to the recovery leader, program administrator, and other internal stakeholders.
- Ensure recovery team members are aware of their roles and responsibilities and that staff and faculty members are aware of the business continuity plan.

USC Central ITS CIO
- Communicate with recovery team planners, leaders, and recovery team members to ensure program compliance, expectations and accountabilities for business continuity/disaster recovery plans.
- Communicate with the decentralized school/department IT administrators relative to IT Disaster Recovery inquiries and guidelines.
- Serve as a subject matter expert to approve or recommend IT disaster recovery strategies that meet university standards.
- Ensure executive level support by communicating with key staff faculty staff and researchers to ensure cooperation and collaborations with all aspects of the BCM program.
- Communicate with schools and departments the information gathering and review protocols for reviewing third party vendors.
3. **DISASTER RECOVERY PLAN KEY ELEMENTS**

Key elements of recovery plans for school or department information technology systems include:

3.1 **System description and architecture**

3.2 **Description of the three IT recovery phases:**

3.2.1 **Activation and Notification Phase** – Activation of the IT DRP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. Once the IT DRP is activated, system owners and users are notified of an outage and a thorough outage assessment is performed for the system. Appropriate IT recovery teams are activated.

3.2.2 **Recovery Phase** – The Recovery phase details the activities and procedures for recovery of the affected system. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities through the restoration of IT components, repair of damage, and resumption of operational capabilities at the original or new permanent location. At the completion of the Recovery Phase, the system will be operational and capable of performing key functions.

3.2.3 **Reconstitution Phase** – The reconstitution phase defines the actions taken to test and validate system capability and functionality. This phase consists of two major activities; validating successful recovery and deactivation of the plan.

During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures may include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing. Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future recovery events.

3.3 **Roles and responsibilities**, including descriptions of the responsibilities of DRP director, DRP coordinator, as well as alternates for both positions.

3.4 Training and exercises will be described and implemented to ensure that affected personnel can carry out IT recovery responsibilities.

3.5 **Responsibilities for plan maintenance and distribution**.

3.6 **Appendices**, potentially including team rosters, contact information, contact information for critical vendors, recovery site procedures, alternate data storage facilities, routine data backup procedures, checklists for key activities, in-depth description of detailed recovery procedures where necessary, and validation procedures.