



How to Create an Operational Recovery Plan

SCOPE AND PURPOSE

The purpose of an Information Technology Operational Recovery Plan (ORP) is to reduce the risks associated with unanticipated outages for critical applications and systems. The plan should include procedures to recover and restore critical applications and systems.

The steps outlined below are applicable to all agencies that operate, manage, or use information technology systems to capture and maintain DMH client protected health information.

1.0 DOCUMENT AGENCY ADMINISTRATIVE INFORMATION

- 1.1 Describe the agency's mission, including the organizational, managerial and technical environments. This section should include organization charts, business functions, and a description of the agency's information technology environment.
- 1.2 Identify the list of sites that are included in your recovery plan (e.g., if your agency includes ORP recovery for another site or organization).
- 1.3 Prepare a communication strategy noting information flow, decision-making, and interrelationship among agency core resources for response, recovery and resumption.

2.0 DESCRIBE CRITICAL BUSINESS FUNCTIONS AND APPLICATIONS

- 2.1 Describe critical business functions and their supporting applications, a designation of maximum acceptable outage timeframes for each application, and the recovery priorities.

3.0 DEVELOP A RECOVERY STRATEGY

- 3.1 Describe the portions of the plan that will be implemented based on various levels of incident severity, for example, minor interruption of service, total service failure or loss of a facility. Recovery strategies should be developed to accommodate a worst-case scenario, loss of service and facility.
- 3.2 Describe the recovery strategy that supports the agency's critical application priorities, including identification and evaluation of alternative recovery strategies. Does the agency contract with an outside source for recovery services? Will the agency's information technology infrastructure be rebuilt at another location? Will a hot or cold site be used?
- 3.3 Alternate recovery sites should be detailed within the plan that includes location, contact numbers and the type of facilities/equipment that will be available.

4.0 DEVELOP BACKUP AND OFFSITE STORAGE PROCEDURES

- 4.1 Prepare detailed procedures to include hardware, software (including version), data file back-up and retention schedules, off-site storage details, and appropriate contact and authority designation for personnel to retrieve media.

5.0 PREPARE OPERATIONAL RECOVERY PROCEDURES

- 5.1 Prepare operational recovery procedures (including manual processes) that support the agency's recovery strategy and provide for the recovery of critical applications within the established maximum acceptable outage time frames. Included would be

the process for recovering the critical data-processing activities, application and data recovery, and the process for suspending non-critical activities and any relocation to an interim (back-up) processing site.

- 5.2 The procedures should be detailed enough so that another trained information technology professional would be able to recover the agency's infrastructure should those with primary responsibility be unavailable during the recovery process. Include a high-level network diagram that includes all critical applications.

6.0 DESCRIBE DATA CENTER SERVICES

- 6.1 For agencies using the services of a data center such as an Application Service Provider (ASP), describe the data center location and services that will be provided during recovery. Include information on any interagency agreements, memorandums of understanding or contracts.
- 6.2 If specific coordination of efforts with the data center is critical to the agency's recovery, those procedures should be included within Section 5 above.

7.0 DOCUMENT RESOURCE REQUIREMENTS

- 7.1 Document the equipment, space, telecommunication needs, data, software, hard-copy references (forms and procedures) and personnel necessary for recovery.
- 7.2 Document resources that will be available at an alternate site.

8.0 DESIGNATE RESPONSIBILITY ASSIGNMENTS

- 8.1 Designate management and staff assignment of responsibilities within the operational recovery plan. Use job titles (rather than the names of individuals) as it lessens maintenance on procedures due to staffing changes.

9.0 PREPARE CONTACT INFORMATION

- 9.1 Develop contact lists, which include the names of individuals, job title and contact information. If home phone numbers are included, the contact lists should be designated as confidential.
- 9.2 Develop contact lists for vendors and outside resources critical to the agency's recovery process.

10.0 PREPARE AN EXECUTIVE SUMMARY

- 10.1 Prepare an executive summary that serves as an overview of the structure of the plan, the procedures for updating (plan maintenance) and distributing the plan, and a description of the agency's test and awareness programs.

11.0 TEST THE PLAN AND DOCUMENT RESULTS

- 11.1 Test the plan and document the results. Examples of testing may include data recovery testing, application recovery and/or full plan testing.
- 11.2 Revise the plan based on the test results. Plan to test on an annual basis using the tests results to continually improve the plan.