

APPENDIX L REGIONAL CENTER DISASTER RECOVERY PLAN

I. ADMINISTRATIVE INFORMATION:

- A. Introduction to Operational Recovery Plan**
- B. Procedures to update and Distribute ORP**
- C. Process to test ORP**
- D. Plans for ORP Maintenance and Updating**

II. RECOVERY STRATEGY AND PRACTICES

- A. Strategies for Managing a Disaster**
- B. Disaster Recovery Scenarios**

III. PROCEDURES FOR DISASTER RECOVERY

APPENDICES

- A. Best Practices**
- B. Lessons Learned**
- C. Disaster Planning Resources**

I. ADMINISTRATIVE INFORMATION

A. Introduction to Operational Recovery Plan

The purpose of this guide is to help Regional Centers plan for and react to a disaster or incident that affects their iSeries (AS/400) business functions. The Regional Center's main purpose is to provide services to the people of California with developmental disabilities, and it is important to ensure a continuity of those services. To that end, this guide is designed to outline the steps that will be necessary to provide essential services in the event of any disruption of information services for an unacceptable period of time. Although it's difficult to anticipate every situation that might interrupt normal processes, a well prepared strategy can aid in responding to any event in order to minimize its impact.

In order to assist Regional Centers, the Department of Development Services has built Disaster Recovery sites at Inland Regional Center in San Bernardino and at DDS Headquarters in Sacramento. Inland regional center has the capacity to host two Regional Centers on Logical Partitions and HQ can host up to four Regional Centers.

B. Procedures to update and Distribute ORP

The effectiveness of this plan can be affected by changes in the environment that ORP was created to protect. Such changes include new equipment, software modifications, regulations/laws, or organizational adjustments that affect critical procedures.

The following procedures ensure the ORP is reviewed and updated regularly.

Intent

Annually, assigned staff reviews the ORP. Proposed changes in the plan are then reviewed as a whole by the Disaster Recovery Planning Team (DRPT) and modified as necessary so that the revised plan may be submitted for review as required.

Procedures

1. The ORP coordinator will appoint a review team to review and update the ORP. If not otherwise specified, the DRPT will serve as the review team.
2. The ORP Coordinator assigns a specific date for team members to respond to proposed changes.
3. The DRPT will revise and integrate changes.
4. The revised plan is then reviewed by all staff and Regional Centers involved in the recovery process.
5. The draft ORP is then tested by the DRPT. The draft plan is then revised to the final form and then submitted to appropriate agencies for approval.
6. Copies of the ORP are then sent to users to replace the previous ORP.

C. Process to test ORP

Testing is an integral part of the ORP. Annual testing is necessary to validate the plan and training of personnel in its implementation.

Intent

The ORP should be tested at each participating Regional Center annually. Testing should encompass three stages of Operational Recovery:

- 1) **Reaction** to the disaster,
- 2) **Restoring** critical business functions, and
- 3) **Recovery** of full systems at primary or new site.

Note: the Restoration and Recovery process will test

- 1) Connectivity to DR site,
- 2) Processing of data, and
- 3) storage and retrieval of data.

Procedures

1. It is suggested that each Regional Center conduct at least one annual test that encompasses each of the three stages of Operational Recovery. Additional tests are suggested if changes in the ORP are significant enough to warrant (i.e. major hardware or software change).

2. Tests are considered review and training exercises, as well as test of the functionality of the plan. The conduct and results of each test are used to amend subsequent revisions of the plan. ORP coordinator (or alternate) serves as the test monitor. If problems or omissions are encountered during a test, staff should treat these as simulations of real problems encountered during a real disaster.
3. The DRPT will stagger Regional Center testing as much as possible so that no Regional Center goes without a test in a fiscal year. Design of tests will not be overly complex and ensure that all critical applications are tested.
4. The test should take place over a limited period of time, preferably a week to ten days. Scheduling should minimize impact on regular regional center operations. If at all possible, current data should be made part of the test.
5. After each test the DRPT will meet as soon as possible to document successes, failures, and lessons learned. A copy of this information will be shared with the Regional Center and other Regional Centers as needed to avoid failures and institute best practices with their ORP. Note: Lessons learned and best practices are documented in Appendices A & B.

D. Plans for ORP Maintenance and Updating

The Department recognizes that any ORP requires continuous attention to ensure it remains up-to-date with technology and regulatory requirements of the iSeries and future iterations.

Intent

The Department conducts studies, analyses, and other design efforts to make the ORP as complete and up-to-date as feasible. To accomplish this, the DRPT will:

- Update the ORP to reflect changes in the Department ORP
- Verify the inventory
 - Hardware
 - Software
 - Data files

II. RECOVERY STRATEGY AND PRACTICES

A. Strategies for Managing a Disaster

Strategies associated with this plan only concern hardware, software, and stored data on the IBM iSeries systems. A disaster need not be a situation that damages or destroys the Regional Center but one that renders the iSeries computer unusable for an extended period of time. The Application Support Team will act in an advisory role to determine if the Regional Center should operate from one of the Disaster Recovery Partitions.

Disaster Recovery involves three general phases:

1. The Regional Center identifies a problem with their iSeries computer and contacts the ORP Coordinator to analyze the situation and determine feasibility of recovering the system onto one of the Disaster Recovery sites. (Ref: Section III)
2. The Regional Center installs iSeries libraries on one of the Recovery sites. The site to be determined at the time of the disaster.
3. Once the emergency is over, the Regional Center will retrieve the libraries from the Recovery partition and return to normal iSeries operations at their own site.

These three general phases occur in every recovery situation; the tasks and people involved will vary according to the nature, scope, and severity of the disaster. The Application Support Staff DRPT is primarily tasked with restoration of critical iSeries functions, but this does not preclude them from assisting in other areas if resources/time permits.

Emergency Control Center

If events warrant, the Director of the Department of Development Services establishes an Emergency Control Center (ECC) to concentrate resources and communications to address a Disaster. The time and place to establish the ECC is at the discretion of the Director of DDS or designee. The Regional Center Technical Support Section (RCTSS) ORP Coordinator will coordinate activities with and, if necessary, through the ECC.

Suspending Low Priority Systems and Applications

The Regional Center management, Director of Department of Development Services, or Deputy Director Information Systems Division may at some point decide to suspend or curtail low-priority activities on the iSeries. This would only be done to ensure processing of critical functions and to facilitate the recovery process of the iSeries systems.

Responsibilities

DDS/RCTSS:

1. Maintain ORP Sites hardware
2. Provide emergency logons
3. Set up Disaster recovery machine (Logical Partitions)
4. Establish, maintain, and coordinate ORP Testing with Regional Centers

Regional Centers:

1. Contact RCTSS when there is a situation involving their iSeries computer
2. Download and install Citrix Web Client onto personal computers (Ref Appendix C)
3. Define Recovery Time Objectives and Recovery Point Objectives prior to Disaster

4. Participate in at least one ORP test each calendar year to maintain personnel proficiency
5. Provide RCTSS with required software licenses for use at the Disaster recovery Site
6. Ensure functionality of any third party software used in coordination with the iSeries operations

Application Software and Data Files

All application and data files on the Regional Center iSeries are backed up on a routine basis. It is also recommended that Regional Centers perform a manual option 22 (system data only) and 23 (user data – for encryption) on the Save menu on periodic basis to aid in the restoration of systems and migration to the ORP site. Also Regional centers will provide a list of software and applicable license numbers for use at the ORP site.

Supplies

It is the responsibility of the Regional Center to ensure they have adequate supplies off site to address their immediate needs following a disaster. Unique check stock, special forms, computers, printers, and other office supplies should be kept at an off-site location.

Relocation of Facilities and Resources

The Regional Center should identify backup facilities or working spaces sufficient to carry out critical functions. In order to operate from one of the ORP sites the Regional Center must have a computer or computers with Internet access and loaded with Mozilla Firefox, Internet Explorer version 8 or 9, or Chrome browser. This option gives Regional Center Operators the flexibility to work virtually anywhere they can connect to the Internet.

B. Disaster Recovery Scenarios

A “Disaster” could mean fire, flood, earthquake, malicious attack, terrorism, or other form of event that compromises normal functioning of critical data processes. This document addresses only the recovery of functions that reside on the Regional Centers’ IBM iSeries midrange computer systems.

It is critical to our consumers that they have continued support in the event of a disaster. RCTSS will provide support necessary to assist any Regional Center to restore their iSeries operations. For purposes of providing support RCTSS has built Disaster Recovery sites that can support remote iSeries operations on Logical Partitions (LPARs). Two are located at Inland Regional Center in San Bernardino, and up to four are available on the Headquarters machine in Sacramento. Each of these LPARs can support one

Regional Center's iSeries operations. It is understood that this is a temporary measure until the Regional Center can restore or recover their lost functionality or infrastructure.

III. PROCEDURES FOR DISASTER RECOVERY

1. It is up to the Regional Center to determine when to contact the ORP coordinator.
The primary contact number for the ORP Coordinator is (916) 653-3329 (DDS helpdesk) during normal business hours (7:00 am – 5:00 pm).
2. The ORP coordinator directs the Regional Center where (Inland or HQ) to send the Regional Center backup tapes.
3. The ORP coordinator issues a block of DDS Citrix logons for the Regional Center.
4. The backup tapes are restored at the Disaster Recovery site by the RCTSS Helpdesk.
5. The Regional Center can begin logging users on the system and continue critical iSeries system operations.
6. Once the Regional Center has regained iSeries system functionality on site, the RCTSS technical support will coordinate a time/date to send data tapes back to the Regional Center for restoration.
7. After the disaster, the ORP Coordinator will convene a lessons learned meeting as soon as practical and include these lessons in an appendix or as a best practice.

BEST PRACTICES:

- 1) Work out an agreement with nearby Regional Centers for temporary workspace. There are many advantages from working at another Regional Center.
- 2) You will also want to consider temporary office space if you cannot work from another Regional Center. This may include some staff simply working from their home.
- 3) Store an electronic copy of critical documents, phone listing, software license keys, etc to a public (but password protected) email address. (Examples: Gmail, Yahoo Mail, Hotmail) During a disaster these documents are available anywhere you can access the World Wide Web.
- 4) If an organization has special print requirements they should keep a limited supply offsite to use in case of an emergency. (Examples: Check Stock, Invoices, Medical forms, State/Federal/Local forms)
- 5) Make sure that your Operational Recovery Plan is not a mystery to staff and that they can readily find information. (Emergency Information card, website, Etc.)
- 6) Plan and execute an ORP exercise each calendar year to maintain personnel proficiency.
- 7) Ensure lines of succession and phone numbers are known to other key personnel and outside agencies.
- 8) Address technology/business changes in ORP and build into testing scenario.
- 9) Key management should take time to participate in drills/exercises.
- 10) Perform an option 22 and 23 save every quarter, have two copies, one for offsite storage, and one in another secure location onsite for easy access.
- 11) Replace tapes every 3-5 years to prevent backup failures.

LESSONS LEARNED:

- It will benefit the Regional Center and DDS personnel to include Regional Centers in the test phase of new technology.
- Spot check to ensure that your backup tapes are saving the data libraries.
- Check nightly backup logs to make sure all critical files have been saved.

DISASTER PLANNING RESOURCES

1. Federal Disaster planning Agency: www.ready.gov
2. Governor's Office of Emergency Services: www.oes.ca.gov
3. Department of Technology Services: www.dts.ca.gov
4. Department of Developmental Services: www.dds.ca.gov
5. DDS/ISD Application Support Team Website:
<http://www.dds.ca.gov/AST/DisasterRecovery.cfm>