State of Oklahoma

<Insert Agency Name Here>

Disaster Recovery Plan Template

Version 1.0

<Date>

TABLE OF CONTENTS

DISASTER RECOVERY PLAN – DOCUMENT CHANGE CONTROL

Date	Version	Requester	Tech. Writer	Change/Review

Modified by: ____ ________/____/_____

Reviewed by: ____ ________/____/_____

Approved by: ____ ________/____/_____

EXECUTIVE SUMMARY

Overview

The following Disaster Recovery plan (**DRP**) and related procedures are for the ***(Agency)***. This plan is intended to restore the operability of designated systems and applications in ***(Agency)***'s data/operations center facility at an alternate location following an incident (or within the existing facility, if it is useable).

The following topics are addressed in the plan.

Plan Distribution

Plan Objectives

Plan Assumptions

- Definitions

Processing Environment

- Scope of Recovery
- Environment Description
- Essential Equipment List

Scripted Recovery Procedures

Recovery Plan Elements:

1. Plan for Major Disasters
2. Roles and Responsibilities
3. Recovery from Major Disasters
4. Recovery Teams
5. Providers
6. Restoration Priorities
7. Media Protection
8. Computer Room Operating Procedures
9. Operating Systems
10. Physical Security and Access Control
11. Software Security
12. Backup Facilities
13. Updating and Maintaining the Recovery Plan

Recovery Statement Summary

(Agency)'s Information Technology (**IT**) group mitigates risks to reduce potential issues and impacts by developing plans that provide the ability to recover from situations including, but not limited to: unplanned evacuations; power outages; major water leaks; fire, loss of water/sewer service; severe weather; and any facilities failures that may cause business interruptions.

Plans are designed to account for business interruptions of various lengths and scopes. The plans require that IT is able to recover critical functions according to their time criticality.

Each critical IT function has a designated leader responsible for preparing and testing its recovery script(s). Each critical IT function also establishes operational guidelines and procedures for disaster recovery to address identified scenarios.

Recovery Scenario #1: The Preferred Solution for a Total Data Center Loss

In the event of a total loss of our data center:

1. The first move will be to the fully equipped ***(Provider Name)*** Hot Site with all the infrastructure and communications services required to resume critical operations within a relatively short period of time (48 to 72 hours).
2. As soon as hardware can be acquired and installed at a Cold Site, processing will be moved from the Hot Site facility to the less costly cold site.
3. All applications will eventually be processed at the Cold Site location, even those not classified as critical.
4. Concurrent with the (hot and cold site) backup facility processing is the reconstruction of the original or a new permanent facility, and the planning for the final move back to this site.
5. By taking advantage of both the hot and cold backup sites as outlined above, IT personnel can restore production operations at their own facility in the shortest possible time following a catastrophic event.

Recovery Strategies: Activities and Time Frames

Short-Term (2 to 3 Days):

1. The first action will be to determine the criticality of the situation, including whether or not to "declare" a disaster condition and activate ***(Agency)***'s Hot Site agreement with ***(Provider Name)***.
2. Once a disaster condition has been declared, the ***(Agency)*** Help Desk will serve as the central point of contact for notifications. This process will start after the Disaster Recovery Coordinator, has notified the appropriate management team to make the declaration official. Following this decision, the ***(Agency)*** Help Desk will begin making the necessary calls to contact everyone in the call chain by priority, using the Emergency Contact list. ***(Agency)*** Management and the disaster recovery team leaders will meet at one of the designated command operation center locations, based on the circumstances creating the disaster situation. Management will select one of the following locations, depending on the conditions following the disaster. The availability of the space to be used may depend on the accessibility of each choice listed below; they are listed in order of preference.
   A. Location alternative 1 (to be specified by the ***(Agency)***)
   B. Location alternative 2 (to be specified by the ***(Agency)***)
   C. Location alternative 3 (to be specified by the ***(Agency)***)
   D. Location alternative 4 (to be specified by the ***(Agency)***)
3. Once the determination has been made to declare a disaster condition and activate the ***(Provider Name)*** Hot Site agreement, the critical path will be to establish wide area network (WAN) connectivity using the designated alternative broadband communication circuits required to connect ***(Agency)*** and other state agencies in Oklahoma to the ***(Provider Name)*** Hot Site facility. If the designated primary or alternative connection point(s), such as the Internet Service Provider (ISP) point of presence (PoP) is no longer available, lead times on new broadband

circuit connections can take 30 to 45 days or more. Broadband circuit provisioning can be shorter or longer than 30 to 45 days, depending on: 1) the specific location(s) in question; 2) the local availability of infrastructure (preexisting copper and/or fiber connections); and 3) bandwidth capacity in the specific area. This is a requirement that needs to be addressed in advance with local providers, such as OneNet, Cox and/or AT&T.

Medium-Term (6 to 12 weeks):

1. Replacement hardware and software may need to be ordered for installation at a temporary facility, preferably a Cold Site.
2. Plans to locate a cold site to house the replacement hardware and software should be made prior to a disaster. Once the cold site is prepared, processing will be moved from the Hot Site facility to the cold site.
3. All applications will eventually be processed at the Cold Site location, even those not classified as critical, until the original facility is restored or rebuilt.

Longer-Term (6 months to 2 years):

1. Once the hot and cold site backup facilities have been established, the reconstruction of the original or a new permanent facility will begin and the planning for the final move back to this site is initiated.

If any one of these strategies is omitted, the minimum recovery time frame will be the longer of those remaining.

Recovery Scenario #2: The Strategy for Loss of a Critical System or Component

In the event of a loss of any critical system or component(s) rendering critical systems unusable:

1. The initial actions will include:
   a. Notify IT management as needed, depending on the severity and impact of the expected outage.
   b. Notify the appropriate IT team responsible for the system or component and begin recovery processes.
   c. Notify IT Help Desk.
   d. ***(Agency)*** Help Desk will notify all affected agencies and entities.
   e. Provide periodic recovery status updates to all parties until the system or component(s) are fully restored.
2. Execute the recovery script for the specific system or component(s) until recovery is complete.
3. Escalate to Providers, IT staff and ***(Agency)*** management, as needed, if standard recovery procedures are not adequate to recover the failing software and/or hardware components involved.
4. Notify ***(Agency)*** Help Desk and ***(Agency)*** management as needed, when the system and/or component(s) have been restored and tested for return to production use.
   a. ***(Agency)*** Help Desk will notify all affected agencies and entities when operational status has been restored.

Summary

Continuity of Business Operations requires two distinct planning and recovery components. One component is the Disaster Recovery plan, which addresses all technology processes required to

support critical business functions. The other component is the Business Continuity plan, which is separate from the Disaster Recovery plan; it addresses the continuation of critical business operations with or without the availability of technology systems.

In the event of an actual disaster, ***(Agency)*** will execute it DR plan utilizing the Hot Site recovery services of ***(Provider Name)***, which will include all the equipment needed to restore processing capability and to reestablish network communications within 2 to 3 days.

These procedures must be fully tested to verify if critical components and/or procedures are identified and recoverable. This will remain an uncertain risk until such time that the recovery procedures defined and developed have been tested. Each recovery function must be tested individually (component tests) at least once; and again collectively for the most critical functions, including critical platforms and scenarios. Additional testing is necessary on a periodic basis (at least annually and/or after major changes are made to the business or technology environments).

INTRODUCTION

This document includes the disaster recovery plan (**DRP**) and related contingency requirements for the ***(Agency)***. It consists of detailed written practices and procedures to mitigate interruptions to "critical information systems" and/or the "loss of data and services" from the effects of natural or man-made disasters. This DRP applies both to major, usually catastrophic, events that deny access to the normal facility for an extended period, and to less catastrophic events that may deny access to only portions of the facility or certain systems. The DRP is an IT-focused plan and therefore may also be referenced as a Technology Recovery Plan which has been designed to restore operability of the designated systems and applications in ***(Agency)***'s data center facility at an alternate site (or within the existing facility if not a total loss) after an emergency.

This DRP was developed by ***(Agency)***'s Information Technology (IT) group.

Below is a reference from the statewide INFORMATION SECURITY POLICY – DEFINITIONS & STATED REQUIREMENTS, which specifies the *state-wide policy* minimum baseline requirements expected for Disaster Recovery plans.

INFORMATION SECURITY POLICY – DEFINITIONS & STATED REQUIREMENTS

8.2 Disaster Recovery Plan

8.3 Business Recovery Strategy

PLAN DISTRIBUTION

Hard copies of the DRP are stored at various office facilities and at alternate locations (sometimes at employees' residences). Copies are maintained at the data center and with members of the recovery team, including:

IS/IT Director's Home
Operations & Applications Manager's/**Disaster Recovery Coordinator Primary** Home
Systems & Operations Administrator's Home
Applications Development Administrator's Home
Networks, PC's & Servers Administrator's Home
Information Security Officer's/**Disaster Recovery Coordinator Alternate** Home
Help Desk Manager's Home
Contracts & Purchasing Administrator's Home
Other team captains' and alternates' Homes (as needed)
Computer room
Offsite storage
Backup recovery site (once one has been identified)

The master copy of the DRP is maintained on an IT file server and is backed up nightly. Printed and electronic copies are stored in a secure location offsite. Having copies of the DRP at various residences is intentionally redundant. This will save time during recovery, by avoiding printing multiple sets of the plan and distributing the copies.

PLAN OBJECTIVES

The overall objective of this DRP is "to protect ***(Agency)***'s assets and employees and to safeguard the agency's vital records". IT is the custodian of ***(Agency)*** information processing assets and must guarantee the continued availability of essential Information Technology (**IT**) services. The goal of this DRP is to document the pre-agreed procedures for responding to a disaster involving a partial or total loss of the data center and its services.

A disaster is defined as the occurrence of any event that causes a critical disruption in IT capabilities. The purpose of the DRP is to mitigate the effects a disaster will have upon on-going operations. This DRP addresses the most severe disaster, requiring relocation to an alternate facility, as well as occurrences of a less severe nature. Occurrences of a less severe nature are controlled at the appropriate management level as a part of the DR Plan.

This DRP will be distributed to all recovery team members. All recovery team members will receive updates whenever they are made to this DRP. The general approach is to make this DRP as threat-independent as possible. This means it must be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the DRP is organized around a team concept. Each team has specific duties and responsibilities, once the decision is made to invoke the disaster recovery mode. The captains of each team and their alternates are key IT personnel. This DRP represents a dynamic process that is kept current through updates, testing, and reviews. As recommended changes are completed or as new areas of concern are recognized, the DRP will be updated reflecting the current status.

PLAN ASSUMPTIONS

The definitions below are provided to clarify the different types of contingency planning and contingency plans. This document only addresses the Disaster Recovery Plan and is the result of ***(Agency)***'s Disaster Recovery Planning project. A Business Continuity Plan is included in a separate document.

Definitions

- Disaster Recovery Planning is the technological aspect of contingency planning. It is the advanced planning and preparations necessary to minimize loss and ensure continuity of the critical technology functions of the agency in the event of disaster.
- Disaster Recovery Plan (**DRP**) is the document that defines the resources, actions, tasks and data required to manage the business technology recovery process in the event of a business interruption. The plan is designed to restore the technologies required to support critical business processes within clearly stated disaster recovery goals.
- Disaster Recovery (**DR**) is the process of responding to an interruption in services by implementing the disaster recovery plan to restore the agency's critical business technology functions. This includes the tasks and activities designed to return the agency to an acceptable operational level.
- Business Continuity Planning is a process that identifies potential impacts that threaten the business operations of our agency. The deliverables from this process provide a framework for building resilience, with the goal of mitigating risk by planning an effective response that safeguards the interests of the agency.

- Business Continuity Plan (**BCP**) includes written practices and procedures to mitigate interruptions to "business activities and business processes" from the effects of major business failures resulting from natural or man-made disasters. The BCP focuses on sustaining an organization's business functions during and after a disruption.

Worst Case Disaster Scenario: This DRP assumes that an event has crippled or partially crippled the data center, possibly forcing ***(Agency)*** to reestablish full operations at an alternative facility.

Proposed Recovery Scenario: In the event of total loss of the data center:

1. The first move will be to a fully equipped Hot Site with all the infrastructure and communications services required to resume critical operations within a relatively short period of time (24 to 48 hours).
2. As soon as hardware can be acquired and installed at a Cold Site, processing will be moved from the Hot Site facility to the less costly cold site.
3. All applications will eventually be processed at the Cold Site location, even those not classified as critical.
4. Concurrent with the (hot and cold site) backup facility processing is the reconstruction of the original or a new permanent facility, and the planning for the final move back to this site.

By taking advantage of both the hot and cold backup sites as outlined above, IT personnel can restore production operations at their own facility in the shortest possible time following a catastrophic event.

PROCESSING ENVIRONMENT

Scope of Recovery

The operational environment of the ***Agency Name*** includes services from the following general-support and critical-function systems. These systems and services are supported and maintained by the Information Services Division. The following sections describe the environment and list essential systems and functions provided by ***(Agency)*** as statewide and agency specific services. These are the services to be restored.

Environment Description

(Agency) is made up of multiple divisions. These divisions should be described in this section with regard to the environment that they run in (Novell for example), workstations and servers in each division, and functional areas within each division.

Essential Equipment

The follow is a list of the essential equipment required for ***(Agency)*** services with recovery ratings:

Functional Area Team Name	Equipment Description	Recovery Rating	Recovery Priority
Network Team			

Functional Area Team Name	Equipment Description	Recovery Rating	Recovery Priority
Voice Communications Team			
File Server Team			
PC Team			
Internet Team			
Systems Programming Team			
Computer Operations Team			

Disaster Recovery Scripts

The following lists the DR scripts for each of the essential systems identified above:

Disaster Recovery Scripts		Script Received	Table Top (TT) Test	TT Test Review & Revisions	Acceptance Form Received	Component (CT) Test	CT Test Review & Revisions	Re Tes
Network Team								
1								
2								
3								
4								
Voice Communications Team								
5								
6								
7								
Internet Team								
8								
9								
10								
Portal Team								
11								
File Server Team								
12								
13								
14								
Desktop Team								
15								
16								

Disaster Recovery Scripts		Script Received	Table Top (TT) Test	TT Test Review & Revisions	Acceptance Form Received	Component (CT) Test	CT Test Review & Revisions	Rec Tes
Enterprise Server Support Team								
17								
18								
19								
20								
21								
22								
23								
24								
Operations Team								
25								
26								
27								
28								
29								
30								
Applications Development & Support Team								
31								
33								
33								
DR Plan Document								
	Totals							
	Percent Complete							

RECOVERY PLAN ELEMENTS

1. Recovery Plan for Major Disasters

The cycle from the occurrence of a disaster to the full restoration of normal processing has four (4) phases:

1) Initial response;

2) Preparation for temporary backup site operations;

3) Backup site fully operational, and

4) Restoration and return to permanent facility.

A. Detection and Reaction

As soon as an emergency situation happens, the on-site personnel must contact the appropriate emergency authorities and then take the necessary steps to minimize property damage and injury to people in the vicinity. Following these procedures, they will then contact the IT Management / Damage Assessment Team so that the team can personally make an on-site evaluation of the disaster.

B. Identifying the problem – Notifying the authorities

i. Emergency services

Telephone the following numbers to reach local authorities for emergency situations such as fire, explosion, earthquake, tornado, etc.:

Functions	Names	Contact Numbers Office	Home	Pager	Cell
Police/Fire/Ambulance		**911**	**N/A**	**N/A**	**N/A**

C. Establishing a Command Center

i. *(Agency)* Command Center for Operations

Once a disaster condition has been declared, the ***(Agency)*** Help Desk will serve as the central point of contact for notifications. This process will start after the Disaster Recovery Coordinator, has notified the appropriate management team to make the declaration official. Following this decision, the ***(Agency)*** Help Desk will begin making the necessary calls to contact everyone in the call chain by priority, using the Emergency Contact list. ***(Agency)*** Management and the disaster recovery team leaders will meet at one of the designated command operation center locations, based on the circumstances creating the disaster situation. Management will select one of the following locations, depending on the conditions following the disaster. The availability of the space to be used may depend on the accessibility of each choice listed below; they are listed in order of preference.

(1) Location alternative 1 (to be specified by the ***(Agency)***)

(2) Location alternative 1 (to be specified by the ***(Agency)***)

(3) Location alternative 1 (to be specified by the ***(Agency)***)

(4) Location alternative 1 (to be specified by the ***(Agency)***)

D. Reducing Exposure

Following the procedures below will help reduce the agency's exposure to additional losses because of actions not taken by on-site personnel. These actions are targeted at emergencies concerning air-conditioning, fire, or electrical or water damage.

i. Air-Conditioner Failure

A graphic temperature-and-humidity monitor may be located in the computer room 24 hours a day. The temperature must be checked each morning and periodically if a heat increase is noticed. The computer room may have multiple air-conditioning units; the fans in the units will normally operate at all times to maintain the proper air flow. If a unit fails, the remaining units can carry the load for most processing, but only for a limited amount of time. The failing unit needs to be repaired as soon as possible to take the strain off the remaining units.
The normal temperature for the computer room is between 68 and 76 degrees. If the temperature rises above 76 degrees, take the following precautions:

(1) Advise the operations shift supervisor that the temperature is above the normal operating range. The operations shift supervisor will notify the maintenance company for corrective action and then notify the Operations Administrator and Operations & Applications Manager.

(2) If the temperature rises above 80 degrees, the Operations Administrator must be notified. The Operations Administrator must decide which non-critical applications may continue to be processed.

(3) If the Operations Administrator decides to power down the computer or if the computer powers down by itself because of excessive heat, it must not be powered up until approval has been received from the Operations Administrator.

(4) Maintenance company personnel will perform periodic maintenance for the air-conditioning units. They will clean the filters, check the coolant, check the belts and hoses, and do normal visual inspections. If any problems occur between scheduled maintenance operations, the maintenance company must be notified.

ii. Fire Alarm Procedures

The fire alarm system can detect fires within the first few seconds. It notifies the local fire department through 24-hour, central-station monitoring. If the fire alarm system has not been activated, but fire or smoke is detected in the computer room, do the following:

(1) Quickly assess the surrounding environment to determine the source of the problem.

(2) If the situation looks manageable, use one of the hand held fire extinguishers to attempt to extinguish the fire. NOTE: Fire extinguishers are mounted on the wall throughout the computer room.

(3) If unable to extinguish the fire and there is time to do the following SAFELY:

(a) Pull the fire alarm.

(b) Call the Operations Administrator, who will call the Operations & Applications Manager and other office management.
(c) Power down all computer equipment.
(d) Exit the data center.

(4) If time permits:

(a) Remove current tapes from computer room to a safe place.
(b) Remove as many tapes as possible.
(c) Retrieve a copy of the DR Plan.

(5) Notify the IT Management / Damage Assessment Team from the Emergency Contact List.

iii. **Electrical Failure Procedures**

The *(Agency)* computer room has battery-powered emergency lighting. It also has a UPS system and backup generator to provide continuous electrical power to the computer room.

Should an electrical problem be detected in the computer room, the following steps must be taken:

(1) Immediately notify the Operations Administrator, who will contact the Operations & Applications Manager.

(2) If the backup generator fails, power-down the computer equipment prior to the UPS system draining.

(3) The Operations Administrator will advise IBM and other hardware Providers as required of the electrical failure.

(4) The Operations Administrator will advise the Database Administrators and Systems Software staff so they can verify that all files are properly restored.

(5) The Operations Administrator will notify the Help Desk of the expected time the system will be up.

iv. Flood and Water Damage.

Water damage can be caused from a discharge or leak in the sprinkler system, broken pipes, bathroom facilities, or the flow of water into the computer room from another area of the building because of fire, etc. The following steps must be followed if there is a water problem:

v. If the Water Damage Exposure Has Affected the Computer Hardware:

(1) Power down the computer equipment.

(2) Notify the Operations Administrator, who will call the Operations & Applications .

(3) The Operations Administrator will contact IBM and other hardware Providers as required to have the equipment checked for damage before the equipment is powered up.

(4) The Operations Administrator will advise the Database Administrators and Systems Software staff so they can verify that all files are properly restored.

(5) The Operations Administrator will notify the Help Desk of the expected time the system will be up.

vi. Evacuation of the Facility.

Employees will be evacuated from the facility if the building is unsafe. Employees will be constantly trained in emergency procedures and will know evacuation routes from various parts of the building. Drills are conducted periodically to refresh the memory of long term employees and give instructions to new employees. The drills inform the employees as to which people are responsible for directing the evacuation and checking that all areas have been properly cleared.

vii. Advising the Management / Damage Assessment Team of the Situation.

As soon as possible after a disaster, notify the Executive Management Team. It is the responsibility of the Operations Administrator or Operations & Applications Manager to make sure the team is advised of the situation. If the on-site person was unable to contact operations management, that person will now be responsible for contacting the Management / Damage Assessment Team. The team members will be phoned in the following sequence until someone is reached. The person reached will continue to call the remaining team members.

Name	Home phone	Work phone
1st contact		
2nd contact		
3rd contact		
4th contact		

The team will personally visit the site and make an initial determination of the extent of the damage. Based on their assessment, all or part of the DR Plan will be initiated. The team will decide:

(1) If the computer operation can be continued at the site and repairs can be started as soon as possible.

(2) If the computer operation can be continued or restarted with the assistance of only certain recovery teams.

(3) If a limited computer operation can be continued at the site and plans started to repair or replace unusable equipment.

(4) If the computer center is destroyed to the extent that the backup recovery facility must be used and the full DR Plan initiated.

(5) The Management Team will decide on its plan of action and then notify senior management. If the action plan requires the assistance of other recovery teams, those teams will be notified.

viii. Creating Workflow Procedures for the Detection and Response

The following section (2) lists the recovery steps in the DR Plan for Phase 1: Detection and Response.

2. Roles and Responsibilities

Heading Name	Executed by	Action Taken
Detection and Response	Operations personnel	Call Operations Management
	Operations Supervisor	Call Emergency Services
Reducing Exposure	Operations personnel	Follow Emergency Procedures for fire, electrical failure, or water
	Operations Supervisor	Power down computer equipment and air-conditioning, contact maintenance, minimize water damage by covering equipment
Evacuation	All occupants	Leave building
Advising Emergency	Operations personnel	Call emergency services as required – Section 2-B.
Management Team	Disaster Recovery Coordinator	Assess damage, etc. – see sections below

A. Management / Damage Assessment Team: Initial Response

i. Coordinate initial response following procedures to protect life and minimize property damage.

(1) Assess the damage.

(2) Determine extent to which DR Plan will be utilized.

(a) Minor Damage— Processing can be restarted in a short time with no special recall of personnel.

(i) Anticipated downtime is less than one day. Damage could be to hardware, software, mechanical equipment, electrical equipment, or the facility.

(b) Major Damage— Selected teams will be called to direct restoration of normal operations at current Site

(i) Estimated downtime is two to six days. Major damage to hardware or facility.

(c) Catastrophe— Damage is extensive. Restoration will take upwards from one week. Computer room or facility could be completely destroyed. All team leaders will be called to begin a total implementation of the DR Plan.

(3) Notify senior management and Help Desk

(4) Notify users at all affected agencies

(5) Prepare regular status reports for senior management

(6) Notify users and Help Desk of projected time for becoming operational

ii. Initiation of Backup Site Procedures

This section will be addressed after a backup site has been selected.

iii. Management / Damage Assessment Team Notifies Other Teams

Following an emergency at the computer center, the operational personnel on site will take the appropriate initial action and then contact a member of the Management / Damage Assessment Team starting with the first name on the list. When a member is located, that member will contact the remaining members of the Management / Damage Assessment Team. The members will meet at or near the disaster to make a firsthand assessment of the damage. They will determine the action to take and will notify senior management. If a determination is made to notify all other Disaster Recovery teams, the Management / Damage Assessment Team will phone the other teams. A brief message will be dictated over the phone and the called person will write down the message. At the end of the message, the called person will read back the message to verify that all critical information is stated.

This same procedure will be used for all calls. It will ensure that all contacts have the same information. Section B (below) contains the list of Disaster Recovery teams and the names of all team members and their phone numbers.

(1) Establish Command Center

The first task for the Management / Damage Assessment Team is to establish a Command Center. The location of the Command Center will be in close proximity to the data center or the Hot-site or Cold-site depending on the nature of the disaster. It could be in a nearby office building or hotel/motel, or in the Hot- or Cold-site. The Command Center must be able to maintain communications with other departments in the agency during the disaster period. The phone number must be made available to all departments and users so that all information can be channeled through the center.

iv. Begin Disaster Recovery Team Operations and Disaster Recovery Logs

The captain of each Disaster Recovery team will document the team's activity by posting it on the Disaster Recovery Log. This will be used by the Management / Damage Assessment Team to prepare status reports for management and will become a historical document for

the agency. The Management / Damage Assessment Team will also use the log to coordinate the concurrent activities of the various teams.

B. Disaster Recovery Teams — Emergency Contact List

		Contact Numbers			
Functions	**Names**	**Office**	**Home**	**Pager**	**Cell**
Executive Management Team					

Management / Damage Assessment Team				
Captain: Primary DR Coordinator				

Information Security Team				
Captain: Primary BC & Secondary DR Coordinator				

Computer Operations Recovery Team				
Captain				

Systems/Database Software Recovery Team					
Captain					

Applications/Database Software Recovery Team					
Captain					

		Contact Numbers			
Functions	**Names**	**Office**	**Home**	**Pager**	**Cell**
Network Recovery Team					
Captain					
Network Server Recovery Team					
Captain					
Desktop Computing Recovery Team					
Captain					
CORE					
Captain					
Communications Recovery					
Captain					
State Portal Recovery					
***(Agency)* Help Desk**					
Captain					
Police/Fire/Ambulance		**911**	**N/A**	**N/A**	**N/A**
Civil Emergency Management		**521-2481**	**N/A**	**N/A**	**N/A**
(Air Conditioning Service)					
***(Agency)* Functional Area Managers**					

		Contact Numbers			
Functions	**Names**	**Office**	**Home**	**Pager**	**Cell**

3. Recovery Plan for Major Disasters

A. Establishment of Full Recovery at Backup Site

i. All planned software and resources are identified and compatible hardware is in place at a backup site, and the applications must be tested.

ii. Communications network and other equipment are in place to be fully operational.

Make arrangements with the telephone company and other communications Providers for delivery and installation of temporary equipment. Providers that specialize in used equipment can deliver their equipment in a very short time. Conduct a complete series of tests to ensure full recovery of the communication network capabilities. Provide for full restoration of service at the original or new alternate facility.

B. Disaster Recovery Team Checklists

The checklists in Appendix B (Form 21) are to be used by each team captain to keep track of the many activities that will be performed simultaneously by their team. The Management Team will collect these checklists and prepare a detailed report of daily progress. The lists will also be used to coordinate all events from the Command Control Center.

C. Restoration of Facilities and Operations at the Original and/or Alternate Site

With the backup facility functioning as the data center, it is time to turn attention to either moving to the Cold-Site and/or rebuilding the permanent data center. Reconstruction plans should already have been in progress, but now it is time to devote more effort to this area. The full reconstruction is normally a two-step process. The first step is to use a cold-site as a replacement of the high-cost, hot, backup site. The permanent replacement hardware that will eventually be used at the permanent facility is ordered and installed at the cold-site. Once it is tested and operational, the production processing is moved from the hot backup site to the now-operational cold-site. Many hot sites also provide both a hot backup site and a cold-site. Reconstruction at the permanent facility may not require a totally new building but only repair of the existing facility. Once the permanent facility is ready for use, the hardware at the operational cold-site can be moved to the permanent facility.

4. DISASTER RECOVERY TEAMS

A. Emergency Contact List in Section 2-B & Activity Checklists Provided in Section 3-B

See the sections named above to view these resources.

B. Description and Responsibilities

i. Disaster Recovery Coordinator

The manager of Operations and Applications has been given the responsibility of Disaster Recovery Coordinator and will coordinate the activities stated in this DRP. The manager of Information Security is the Alternate Disaster Recovery Coordinator.

Part of the DRP maintenance process requires the coordinator to monitor information that needs to be updated in the plan. As people are assigned new duties, their names, addresses, and phone numbers have to be entered in the DRP; when the procedures, addresses or phone numbers change, the master copy of the DRP is updated, and updated copies are distributed electronically, either on CD's or USB drives. Updated hard copies of the DRP must also be distributed to the appropriate staff and offsite locations.

All activities in the DRP need to be tested. This not only ensures that the procedures work, but also acts as a training exercise for the various teams. The Coordinator will schedule testing and document the success or failure. He or she will prepare reports for management and for the state Auditor when required. When tests fail, the coordinator will work with the appropriate team captains to resolve the problems and schedule another test.

As hardware, software, and communications are updated at the data center, the coordinator will communicate with the hot backup site to ensure that it can adequately support all critical systems.

ii. Management / Damage Assessment Team

Team Captain: Operations & Applications Manager_____

Alternate: Contracts/Purchasing Manager_____

Responsibilities:

(1) Supervise the initial reaction to the disaster and ensure that organizational property and lives are secured.

(2) Review the damage and notify the appropriate state authorities.

(3) Provide detailed accounting of the damage to senior management (see section 2-B).

(4) Determine to what extent the Recovery Plan will be implemented.

(5) Initiate recovery process.

(6) Call team captains and begin executing the disaster recovery plan.

Team Members:

Refer to Section 2-B.

Disaster Recovery Functions:

(1) Set up a Control Center per the instructions of the DRP so that all operations will be channeled through one area.

(2) Distribute the new phone number(s) to all teams and emphasize the use of the phone only for necessary information.

(3) Notify the backup facility of planned intention to use it.

(4) Start using the Disaster Recovery Logs for all operations.

(5) Supply senior management and the Help Desk with scheduled updates on status.

(6) Notify all users of the status of the computer facility.

(7) Arrange for any additional professional help.

(8) Coordinate interviews to fill any vacancies.

Salvage Functions:

(a) Contact Risk Management and do follow-up as required.

(b) Review the damage and determine hardware that can be repaired.

(c) Prepare report that details damage and outlines disposition.

(d) Initiate replacement process (Provider contacts, etc.)

(e) Advise other teams of the replacement provisions in existing contracts, if any.

iii. Operations Team

Team Captain: Systems Software and Operations Administrator _____

Alternate: Networks, PC's & Servers Administrator_____

Responsibilities:

(1) Restore files and applications and operate systems at the hot backup site.

(2) Prepare operations schedule at hot backup site.

(3) Coordinate activities necessary to restore facility at the existing or new permanent location.

(4) Order and install computer hardware necessary for normal processing at permanent location.

Team Members:

Section 2-B describes the teams and emergency contact lists.

Disaster Recovery Functions:

(1) Computer operations

(a) Operate or give assistance to computer operator at hot backup site.
(b) Obtain backup tapes and restore files at hot backup site.
(c) Verify restoration process to ensure integrity and continuity.
(d) Audit financial files with functional users to ensure recovery process was complete.
(e) Determine restart point for critical systems.
(f) Test critical systems for production processing.
(g) Establish an operations schedule at hot backup site.
(h) Inform users of processing schedule at hot backup site.
(i) Arrange for shipment of backup supplies to hot backup site.
(j) Arrange for shipment of backup tapes from hot backup site to off-site storage.
(k) Monitor controls and security during recovery mode.

(2) Facility preparation
(a) Coordinate the repair or construction of the new permanent facility at the original location or new location.

(3) Replacement hardware
(a) Contact hardware Provider to determine if current hardware is repairable. If hardware must be replaced, get proposed time-frame for delivery. If time-frame is not satisfactory, get proposal from used-hardware Provider.
(b) Check on requirements for cables, connectors, and other start-up requirements.
(c) Arrange for procuring any other data-handling equipment.
(d) Schedule testing with maintenance personnel (Providers, electricians, UPS, etc.).

(4) Cold/Hot site preparation
(a) Periodically review cold/hot-site facility to verify that the environment can support the hardware that will be temporarily operating there (interim equipment may not exactly match original configurations).
(b) Provide for adequate power, cables, and connectors.
(c) Provide for communications requirements.
(d) Provide for security guards and/or limited access to computer room.
(e) Provide for off-site storage.

(5) Computer support equipment.
(a) Determine the need for other support equipment: PC's, printers, paper-handling equipment, etc. Order all required equipment.

(6) Supplies.
(a) Review list of requirements.
(b) Contact Providers on Emergency Provider list.
(c) Arrange for shipment of existing supplies or purchase of replacement supplies.
(d) Notify remaining Providers of disaster and give shipping address of backup facility.

iv. Production Output Control/Mail Distribution Team

Team Captain: Systems Software and Operations Administrator_____

Alternate: Networks, PC's & Servers Administrator_____

(1) Responsibilities:

(a) Restore the production output control and mail distribution operations at the backup facility.

(2) Team Members:

(a) Production Output/Mail Distribution Clerk_____

(i) a. Production Output Control/Mail Distribution

1. Notify users of the disaster and advise them of the temporary procedures for picking up output.
2. Arrange for production control output/mail distribution area(s) at backup facility or somewhere close to original facility.
3. Obtain backup van if necessary for making production output deliveries to agencies and establish revised schedules in conjunction with users and Operations.

v. Procurement and Administration Team

Team Captain: Contracts/Purchasing Manager _____

Alternates: Procurement Specialist (Procurement), Secretary_(Administrative)_____

Responsibilities:

(1) Provide procurement and administrative support for the recovery activity.

Team Members: As listed above.

(a) Procurement services

(i) Provide assistance with purchasing replacement computer, office, or other equipment as required.
(ii) Arrange for shipments of material, supplies, and computer equipment.

(b) Administrative services

(i) Provide all necessary administrative services, such as the payment for emergency equipment and issuing critical supplies, etc.
(ii) Arrange hotel accommodations for personnel stationed at the backup site if required.
(iii) Provide for additional office facilities, including furniture, phones, and office equipment.

vi. Systems & Database Software Team

Team Captain: Systems Software and Operations Administrator _____

Alternate: Networks, PC's & Servers Administrator_____

Responsibilities:

(1) Install operating system software at the backup site allowing the minimum required operations and internal communications to be restored.

Team Members:

Refer to Section 2-B.

Disaster Recovery Functions:

(a) System software

(i) Supply the required operating systems as well as other control systems.
(ii) Restore the systems in priority sequence using backup tapes and verifying continuity.
(iii) Work with backup site and Provider technical staff as needed.

vii. Communications (Voice and Data), Networks, PC's & Servers Team

Team Captain: Networks, PC's & Servers Administrator_____

Alternates: Voice Communications Supervisor, Data Communications Supervisor, Servers Supervisor, PC's Supervisor _____,____

Responsibilities:

(1) Full restoration of all wide area and local area networks (WANs & LANs) required to provide internal and external communications to and from the Recovery Data Center.

(2) Full restoration of essential servers for Data Center processing

(3) Installation of PCs required for Recovery Teams, followed by next priority areas identified in plan.

Team Members:

(a) Voice & Data Communications Supervisors/Team Leads

(i) Determine damage to communications network and establish requirements for replacement equipment.
(ii) Work with the telephone PBX and communications Providers and service providers to restore full service and order additional telecommunications equipment and facilities as needed.
(iii) Notify and inform users and the Help Desk of disruptions in service.

(b) Server Supervisor/Team Lead

(c) PC Supervisor/Team Lead

Disaster Recovery Function: Network, Server & PC Restoration

(a) Supervise restoration of required network components and service provider connections.
(b) Supervise restoration of required servers and functional software.
(c) Supervise restoration of required PCs and required functional software.

(d) Run tests and verify required functionality. Ensure that future processing is accurate by working with recovery team.

viii. Application Development Team

Team Captain: Applications Development Administrator _____

Alternate: Database Administrator_____

Responsibilities:

(1) Ensure production systems are restored and verify continuity of ongoing processing.

Team Members:

(a) Applications Development and DBA staff

Disaster Recovery Functions:

(a) Application systems restoration and recovery

(i) Coordinate with Operations to verify proper restart point.
(ii) Verify application software programs and libraries.
(iii) Supervise file restoration and ensure continuity of data by testing and comparing results to users' listings.

(b) Application programs

(i) Supervise the processing of critical applications at backup site or arrange for processing at service bureau.

(2) Full restoration of the database and verification that the files are current.

Team Members:

(a) Data Base Administration personnel

Disaster Recovery Function: Database Restoration and Integrity

(e) Supervise restoration of the databases from backup tapes.
(f) Restore intermediate data to allow files to be updated to a current status.
(g) Run tests and check them against user listings. Ensure that future processing is accurate by working with users.

C. On-going Functional Responsibilities

i. Disaster Recovery Coordinator or Alternate

(1) Keeps DRP documentation updated; correcting names, addresses, and telephone numbers.
(2) Ensures DRP is properly distributed to team members.
(3) Develops testing schedule of all phases of DRP.
(4) Works with auditors to validate procedures when audited.
(5) Distributes literature on safety and disaster recovery.

(6) Periodically checks backup facilities.
(7) Formally updates DRP every six months using input from teams.

ii. Management / Damage Assessment Team (periodically as needed in response to the situation)
(1) Team leader schedules quarterly meetings, discusses current status.

iii. Operations Team
(1) Keeps computer room floor plans current for both main location and backup facilities.
(2) Keeps copy of all IT hardware configurations.
(3) Keeps updated information on Providers who supply hardware, software, communications, supplies, and custom forms.
(4) Keeps current emergency procedures for fire, water damage, and other potential hazards.
(5) Keeps off-site backup tapes current.
(6) Keeps Operations run-book information stored off site.
(7) Keeps recovery plans operational.

iv. Production Output Control/Mail Distribution Team
(1) Keeps a current listing of backup tapes stored off-site.

v. Procurement and Administration/HR Team
(1) Keeps current listing of Providers to be used in emergency.
(2) Keeps Organization Charts current.
(3) Sets up plans to deal with distribution of emergency equipment and supplies.

vi. Systems & Database Software Team
(1) Ensures operating system and database software copies are kept off site.
(2) Keeps current list of disk files and layout identification.
(3) Prepares a full recovery capability using off-site backup tapes.

vii. Communications (Voice & Data), Networks, PCs and Servers Team
(1) Ensures communications network information is current, including voice and data communications service providers, routers, switches, firewalls, and related equipment required.
(2) Maintains Server and PC hardware and software inventories
(3) Ensures server off-site backup arrangements are complete.

viii. Application Development Team
(1) Reviews all systems to ensure adequate arrangements for off-site backup have been provided for programs, files, and documentation.
(2) Verifies that proper retention is being maintained as noted in retention policy in agency records.
(3) Lists all systems, users, processing priority, and responsible programming staff.
(4) Identifies critical systems and prepares detailed recovery plans.
(5) Ensures database off-site backup arrangements are complete.

ix. Risk Management Team
(1) Reviews risk coverage and verifies adequacy of DRP.

(2) Reviews coverage to verify that risk management coverage is in conjunction with DR Plan

x. State Audit Team
(1) Reviews Recovery Plan to gain a thorough understanding, checks for control points, and verifies for completeness as required.

5. Providers

The following information is documented in an Excel workbook named "***(Agency)***-DR Documentation", which is included in Appendix "A" under the "Operations Team" category.

Not all of the Providers that actively work in the normal business environment will be listed in this section. This section is designed to identify only those specific Providers who need to be contacted to repair or replace equipment or supplies critical to the operation of the data center and required as part of the recovery effort.

Information on Providers includes names and addresses of key sales representatives and technical personnel and lists of all local and central emergency phone numbers.

A. New and Used Hardware Providers

Recovery planning efforts are focused on computing equipment. Detailed descriptions of all installed hardware are maintained. A list of used equipment Providers and their specialties is maintained in the ***(Agency)*** DR Documentation Workbook.

B. Software Providers

A complete inventory of any special software, whether operating system or application system is maintained in the ***(Agency)*** DR Documentation Workbook and a copy kept in offsite storage. All software is backed up on an ongoing basis as part of the DR procedures.

C. Communications Providers

Communications facilities are also a focus of recovery planning with emphasis on reducing the amount of lead time to restore communications. Detailed descriptions of all installed communications lines and equipment are maintained in the ***(Agency)*** DR Documentation Workbook. A list of Providers and their specialties is maintained.

D. Special Equipment Providers

Detailed descriptions of old, unique, or obsolete equipment are maintained. Planning is ongoing to migrate applications off of this equipment.

E. Providers of Office-Support Equipment

A list of office equipment is maintained. A list of office equipment Providers is maintained as part of the state-wide contracts in place with the Department of Central Services.

6. PRIORITIZE ALL APPLICATIONS

A. Rate All Systems with Their Priorities

The principal role of IT is to quickly restore service for critical applications when there is a serious failure or disruption of regular operations because of fire, natural hazards, power

failures, or other causes. Critical systems are identified and prioritized. This is maintained through ongoing Business Impact Analysis and Business Continuity Planning.

7. MEDIA PROTECTION

A. Protection and Retention of Vital Records

The protection and retention of vital records is an IT normal business operation. Various records are made available to state agencies and the public upon request to verify the information the agency supplies as part of their business. State agencies also have legal responsibility to protect certain records for a specified number of years.

Magnetic tape is commonly used to store agency records because of the amount of data that can be contained on a tape cartridge and because the tape can be easily secured in an off-site location.

Some records need to be stored in their original form. The IT data center provides a secure storage area for agency hard copy records.

The data center normally backs up data to magnetic tape cartridge(s) and transports them to the off-site location. Backup processes are scheduled by application and platform. See section C below for backup procedures.

A written procedure and schedule for pickup and delivery by the Production Output/Mail Distribution Clerk is maintained as part of this operation.

B. Protecting Databases

i. Database backups
Incremental backups are completed daily and full disaster recovery backups are completed weekly. Backup tapes are stored off site.

ii. Updates
Transaction logs are generated continuously and backed up each night with the incremental backups so that databases can be recovered to a particular point in time if required.

iii. Database definitions
Database definitions are backed up weekly with the full disaster recovery backup and stored off site.

iv. Software modification source code
Software modification source code is stored on a source code file. The source code file is backed up weekly with the full disaster recovery backup and stored off site.

C. Standard Backup Procedures

A copy of these procedure(s) are in the Appendix in a document named "***(Agency)***-DR Documentation Workbook—this workbook includes to worksheets named [Infrastructure Backup Schedule (GF)] and [Infrastructure Backup Procedures and Host Recovery Validation".

IT creates incremental backups of databases daily and full backups weekly. Backup tapes are rotated to off site storage. The tapes rotated off site are as current as the daily or weekly processing that created them.

D. Off-Site Storage and Go Boxes

i. Go Box Allocation and Contents—a Go Box is used to store backup copies of media (tapes, CDs, DVDs, etc.) and procedural documentation (including recovery scripts), as well as other equipment needed to restore applications and data to an operational state. There should be separate Excel workbooks containing an inventory of each Go Box for each of the following groups:
(1) Applications
(2) Networks
(3) Servers
(4) Desktops
(5) Voice
(6) Admin-Management

ii. Off-Site Storage Location
IT has an off-site storage facility. Backup tapes are rotated periodically (daily, weekly and/or monthly as needed). This process may be fully or partially automated; some inventories may be maintained manually.

Storage Facility Name
address

Phone

E. Application System and Program Documentation

IT maintains documentation on all production applications for which it is responsible. Copies of this documentation are maintained in the off-site storage facility and updated as required.

F. Imaging Procedures

Certain printed reports are generated as an image or non modifiable file and stored in a database. Imaged data is stored on hard disks or CD's. They are also backed up to tape.

G. Personal Computer File Backup

Files critical to the operation of the agency are typically shared by more than one person and are stored in folders on a central file server. These files are backed up daily to tape and rotated off site.

8. COMPUTER ROOM OPERATING PROCEDURES

A. Power-Up Procedures

See Appendix

B. IPL Procedures

See Appendix

C. Power-Down Procedures

See Appendix

D. Schedules (Production Run Schedules)

See Appendix

E. Operations Run-Books

See Appendix

F. Application Responsibility (On-Call Lists by Functional Area)

See Appendix

9. OPERATING SYSTEMS

A. Software Operating Environment

Processing at the backup facility will be under the same operating systems used at the IT Data Center. Computer hardware at the backup facility will be compatible with current hardware.

B. Listing of All Purchased Software Packages

All purchased software will execute at the backup facility. This will be tested periodically.

C. Disk Drives and File Layouts

Disk storage at the backup facility must be compatible with disk storage at the IT Data Center. Restoration of backup files will be tested periodically.

10. PHYSICAL SECURITY AND ACCESS CONTROL

(Agency) maintains a ***(Provider Name)*** security cardkey access system. This system is maintained, monitored and operated locally by IT Operations staff with oversight from the Information Security Office. Further security is provided by personnel located at the reception/administrative desk of each building and/or at the reception/administrative desk of each floor and/or department. Once individuals pass the human element, their access to various areas is controlled by the ***(Provider Name)*** access control system, which prevents unauthorized persons from entering secured areas. Access for the people in the following categories must be stated so that only those persons having the proper authority can enter the various restricted areas:

A. Computer Operations

B. IT Staff

C. Service and Maintenance Personnel

D. Outside Company Personnel

i. Hardware

ii. Communications

iii. Miscellaneous

E. Access Control

Refer to the ***(Agency Name)*** IS/IT Operations and Security Policy (including Physical Security Policy)

F. Computer Room

G. Non-office Hours

H. Physical Security Roles: OHP, etc.

In the event of an incident requiring physical security assistance or law enforcement support, Capitol Security must be contacted.

I. Office Security

Access to the general office areas is normally given to all employees. Certain areas are restricted to normal business hours access only.

11. SOFTWARE SECURITY

A. Sign-On Passwords

See ***(Agency Name)*** IS/IT Operations and Security Policy — Access Control Policy.

B. Maintaining Application Programs

See ***(Agency Name)*** IS/IT Operations and Security Policies for Systems Development Lifecycle and Change Control.

C. Password Maintenance

See ***(Agency Name)*** IS/IT Operations and Security Policy — Access Control Policy.

12. BACKUP FACILITIES SCENARIO

The “Assumptions of the Disaster Recovery Plan” section recommends a fully-equipped hot site facility and a cold site as part of the disaster recovery plan. This is most cost-effective if it becomes necessary to move off site. The recovery will start at the fully equipped facility while preparations are being made to install replacement equipment at the cold site. When the cold site is prepared, the computer operations can be moved from the higher-cost, fully equipped facility to the less expensive cold site. When the permanent facility is reconstructed, the operations can be moved from the cold site to the permanent facility.

A fully equipped (hot site) backup facility is needed for rapid recovery and used for testing operating systems and other critical applications to ensure an efficient and effective recovery with minimal impact on the users. Fully equipped facilities are available to paid subscribers for their use to schedule testing of their operating systems and applications.

A cold site facility (empty computer room that is equipped with raised floor, air-conditioning, electric power, communications facilities, fire protection system, and ready for installation of computer hardware) is the secondary recovery location. Many hardware Providers will try to help out in an emergency situation, but locating and delivering hardware could still take as

much as 6 to 10 days. After delivery, the Provider must still install and test the hardware before turning it over for testing.

A. Subscribing to a Backup Facility

There may be multiple fully equipped backup facilities from which to choose. For the most part, they offer the same services. They may differ in the amount of floor space they offer, the type and size of hardware that is installed, the physical security they have for their facility, or their geographical location, but they still offer the basic solution: an operational computer ready to be used by one of their subscribers. Before choosing one facility over another, ***(Agency)*** will compare their services, location, and hardware, and select the facility that best meets the needs of the agency.

The contract will contain many of the following items: terms and effective date, definition of contract terminology, use of the facility, fees and payment schedule, conditions concerning multiple disasters, liability, hardware changes, confidentiality, and termination of contract.

B. Facility Layout

The disaster recovery company typically furnishes a layout of their facility. This would include the computer room, tape storage room, office area, conference room, reception area, etc.

C. Hardware and Software

Some facilities have multiple hardware configurations. ***(Agency)*** will subscribe to the hardware that meets the agency's needs. ***(Agency)*** will restore its own operating systems on compatible hardware at the recovery facility (hot site). Databases, middleware and similar subsystem software and applications will also be restored.

D. Communications

Communications from the backup facility to the network cannot be effected without planning and testing. If communications providers need to install new lines in order to connect the backup facility to other remote network points, it could require weeks of delays. Preplanning with the providers and having some communications facilities already installed in the backup facilities (hot or cold site) will expedite the connection of any necessary lines. Many backup facilities have preinstalled network bandwidth available as an option in their contract. Major phone companies also offer disaster recovery options (DRO) for a fee that will guarantee that remote network connections will be moved within a pre-established time frame.

Hardware (switches, routers, firewalls, etc.) installed between computer(s) and communications (local and wide area) networks will be pre-installed at the backup facility and connected with its computer(s). In an emergency a link can then quickly be made to ***(Agency)*** and other agencies network locations.

E. Testing

Plans must be tested on several levels to ensure readiness in the event of a real disaster. The data center, as well as the backup facility, is continually being upgraded. New software and hardware are being added, and an application that tested successfully in the past may not execute now. The only way to be assured operational plans and procedures are complete is to utilize the backup facility at least once a year.

Testing at the facility must be well documented. ***(Agency)*** must avoid relying on a single key person to bring up the operating system(s) and restoring necessary libraries and files. If a disaster occurs, that key person may not be available to function as he or she did in the testing phase.

(Agency) has adopted a set of DR Test Plan Objectives and Development Guidelines. Please refer to the Appendix to review the test plan development process.

i. Initial testing

Initial testing will be focused on bringing up the operating system(s), testing job control language (JCL) or initial startup scripts, restoring files on backup facility disk drives that could be different from the drives in the data center, testing communications, and testing basic batch job processes that use 3rd party software. Future testing will require testing all applications that are classified as critical to the operations of the agency. ***(Agency)*** will record any failures in testing and make adjustments to the DRP, recovery scripts, etc., to ensure the next tests are successful.

ii. Restoring files and libraries

Restoration of all disk files, databases and libraries will be tested utilizing backup tapes from the off site storage area. ***(Agency)*** will ensure disk drives at the backup facility are compatible and will plan ahead for options to download files, including the amount of disk space required to allocate to work areas, etc.

iii. Testing critical applications

All critical applications will be tested. This is the only way to know if they will execute at the backup facility. ***(Agency)*** will prepare a schedule for testing all critical applications and document the successes and failures.

iv. Testing communications

Communications may be required in testing some of the critical applications. Communications will be tested to ensure all required network equipment and communication lines are functioning properly.

v. Mock disasters

Although testing at the backup facility has to be scheduled in advance, management must approve a surprise test using a mock disaster. With scheduled testing, the IT staff finds out ahead of time which kind of testing is going to be accomplished and they can prepare for it. Mock disasters evaluate the true effectiveness of the DRP.

vi. Testing program compilations

Support at the backup facility for the programming staff is an essential part of the recovery plan. Programmers must be able to access their source libraries, recompile programs, and re-link them. They also need access to all of their programming and debugging aids. Compilations must be tested for all languages used in the existing environment. Test

systems must be available unless management has decided to eliminate the test systems because of a lack of sufficient disk space at the backup facility.

13. UPDATING & MAINTAINING THE RECOVERY PLAN

Once the DRP has been established, there is a continual process of maintaining and updating the DRP to ensure that it is kept current and its recommendations and provisions are being observed. The maintenance responsibility belongs to the Disaster Recovery Coordinator, but the update process is everyone's responsibility. The IT Director has total responsibility for the entire DRP, but his or her full staff must be aware of the contents of the DRP and must notify the Director if any action or lack of action as specified in the DRP is noticed.

The state Auditor and Inspector will also periodically review the DRP. The Auditor's responsibility is not to make policy but to ensure that ***(Agency)*** is following its policy to have a complete and tested DRP.

A. Disaster Recovery Coordinator's Responsibility

To help prevent the DRP from becoming out of date, establish a schedule for formal updates to the DRP (see form below). Scheduled updates are in addition to any other intermediate updates that are entered as they occur. Such as address changes, hardware updates, software purchases, etc. Six months has been determined as the time between formal updates.

Assigned Date	Disaster Recovery Coordinator	Completion Date
__01/01/yy_____	_____	_____
__07/01/yy_____	_____	_____
__01/01/yy_____	_____	_____
__07/01/yy_____	_____	_____
__01/01/yy_____	_____	_____
__07/01/yy_____	_____	_____
__01/01/yy_____	_____	_____
__07/01/yy_____	_____	_____

B. Team Captain's Responsibility

Each Team Captain also has the responsibility to review and update their section of the DRP at least annually (see form below).

Team Captains	Date	Initials
Management / Disaster Assessment Team	_____	_____
Operations Team	_____	_____

Team Captains	Date	Initials
Production Output Control / Mail Distribution Team	_____	_____
Procurement & Administration Team	_____	_____
Systems & Database Software Team	_____	_____
Communications (Voice & Data), Networks, PC's and Servers Team	_____	_____
Applications Development Team	_____	_____
Information Security	_____	_____

14. DISASTER PLAN CHECKLISTS

In addition to the Business Impact Analysis and the Disaster Recovery Plan, the ***(Agency)*** has completed an inventory of the current environment, plus planned improvements. It is essential to have full knowledge of the present situation and known plans for the future. The checklists below serve to identify existing controls, which are already protecting the agency's assets. Other items in the checklists address good business practices and operational procedures.

The DR Plan is intended to be a comprehensive plan. The checklists below have been divided into major categories: General Overview, Data Center Facility, Data Control/Workflow, Computer Room, Tape Library, Applications Development, Systems and Database Software, State Auditor, Backup Facility, and Reciprocal Agreements. Many of the categories relate directly to sections in the DR Plan. After each question is space to answer: "Yes," ''No" or "Work in Progress (WIP)." There is also a place to enter a notation to explain the response or action if planned. Each checklist is designed to be a work list that can be updated as events occur.

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
A. GENERAL OVERVIEW				
1. If a major disaster to the data center occurred today, could the agency survive?				
2. Has an Impact/Risk Analysis been recently completed?				
3. What is the total dollar amount of the agency's exposure?				
4. Have you prioritized all of your programs?				
5. Have you listed the maximum downtime for all of your systems?				
6. Have you listed the objectives of a recovery plan and the assumptions it includes?				
7. Do you have a recovery plan, and is it current?				
8. Does the DRP include backup facilities?				
Hot backup site?				
Cold site?				
Reciprocal agreement?				
9. Does the backup facility inform you when there is a change in hardware or software?				
10. Have you determined the cost of a recovery plan including: Initial cost? Development cost? Maintenance cost?				
11. Has the plan been approved by top management?				
12. Do you have a Disaster Recovery Coordinator?				
13. Is someone assigned to update the plan?				
14. Does the plan use a team approach?				
15. Do you have people assigned to lead each team?				
16. Is the same person assigned to lead more than one team?				
17. Are names and phone numbers updated regularly?				
18. Has the plan been reviewed by the Internal Audit, Security, and Insurance Departments?				
19. Does the plan provide for recovery from a major disaster, and can it be adjusted for a less severe occurrence?				
20. Has the plan been tested using only material stored off-site?				
21. Is the plan tested at least every 6 months?				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
22. Has the plan been updated as a result of the testing?				
23. Have you ever initiated a surprise test?				
24. Does the plan provide instructions for:				
Emergency procedures?				
Organizational structure following a disaster?				
Off-site storage for all recovery material?				
25. Does the off-site storage have 24-hour access, physical security, vaulting, fire protection, and courier service; round trip travel time of less than 1 hour, access only by authorized persons?				
26. Are the tapes secured in a separately controlled room within the secured area?				
27. Is all system documentation, except program listings, kept in fireproof storage when not in use?				
28. Are there written instructions that define the responsibilities that personal computer (PC) users have for backing up and protecting their files?				
29. Have these instructions been given to all PC users?				
30. Have all data center personnel been advised about the confidentiality of all information they work with?				
B. DATA CENTER FACILITY				
1. Are there signs outside identifying the data center?				
2. Is the building protected by security guards, fences, alarm systems, and/or closed-circuit monitoring?				
3. Is wiring for all security and alarm systems passed through conduit?				
4. Do the guards make scheduled rounds of the building?				
5. If no guards are used, are the people responsible for security trained by security professionals?				
6. Has someone been assigned the responsibility for security of the data center, company, or building?				
7. Are security personnel or computer room personnel on site at all times?				
8. Is there card access to the facility and various				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
areas in the facility?				
9. Are identification badges worn by all employees?				
10. Are visitors required to sign in and sign out?				
11. Is there security at the receiving area?				
12. Are there any Office/Building Emergency Booklets published that include:				
Medical emergencies?				
Fire emergency procedures?				
Evacuation procedures?				
Bomb threats?				
Security violations?				
Weather threats?				
Electrical failures?				
13. Has someone been assigned to provide information, instruction, and supervision for the list in Item 12?				
14. Are evacuation route drawings posted in all hallways?				
15. Have all occupants been instructed and trained in emergency procedures?				
16. Are fire drills conducted on a regular basis under the supervision of your local fire marshal?				
17. Is there a written termination procedure that includes a checklist of items to be returned to the company, such as keys, ID badges, card access, etc.?				
18. Are all employees required to take vacation time so others can perform their duties?				
19. Do all areas of all buildings have a fire alarm system?				
20. Has the fire detection and extinguishing equipment been tested and/or inspected in the past 6 months?				
21. Does the insurance company or fire department make annual fire inspections?				
22. Is the storage area for forms and supplies protected with sprinklers?				
23. Are smoke detectors located in the storage area?				
C. DATA CONTROL/WORKFLOW				
1. Are there alternatives for entering input normally keyed on-line?				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
2. Have you made provisions to have keying done on the outside in emergencies?				
3. Is a copy of the keying instructions stored off site?				
4. Is a software package used for keying, and is it available to outside services?				
5. Have arrangements been made to have your affiliates or divisions key your input?				
6. Are all manual procedures performed by data entry/workflow documented and a copy stored off site?				
7. Are source documents batched and controlled by another department?				
8. Are source documents stamped with date, time, and operator after keying?				
9. Are source documents maintained in their original batches for a short time so they can be re-keyed if necessary?				
10. Are source documents returned to the data control department after keying?				
11. Can the data entry/workflow department be reestablished in another location in a reasonably short time if necessary?				
12. Is access to the data control department restricted?				
13. Are all source documents and computer reports routed through this department for control and balancing?				
14. If communication fails for transmitted reports, has an alternate method for sending reports to users been established?				
15. Is this department responsible for the control of check forms?				
16. Is there a written procedure for issuing a supply of blank checks outside the computer room?				
17. Are checks signed by a different person from the person balancing and distributing them?				
18. Can the check signer be replaced overnight?				
19. Is there any special office equipment critical to the operation of the data center, that provisions for a substitute have not been made?				
20. Are backup signature facsimiles secured off site?				
21. Is there a formal custom-form system that identifies all forms, their reorder point, their				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
supplier, and an alternate supplier?				
22. Is a small supply of all critical custom forms maintained on site?				
23. Are there copies of all form specifications and a copy of the final proof maintained off site?				
24. Is a fact sheet maintained on all Providers of office equipment and forms?				
25. Has an alternate point-to-point pickup and delivery been planned for if the primary method is not operational?				
26. Is there an output distribution report form for every printed report defining: number of copies, decollate, burst, method of shipping, recipient name, and recipient phone number?				
D. COMPUTER ROOM				
1. Is access to the computer room restricted?				
2. Are only the computer operators and system administrators allowed to operate the computer?				
3. Is the room protected by Halon, FM-200, CO, or sprinklers?				
4. Are smoke detectors located: In the ceiling?				
5. Under the raised floor?				
6. In the air conditioning ducts?				
7. Will the smoke detectors operate even if there is a power outage?				
8. Are fire extinguishers located at all exit doors?				
9. Are water detectors located under the floor?				
10. Are waterproof covers stored in the computer room for emergencies?				
11. Is a UPS system installed for short power outages?				
12. Is a generator available for extended power outages?				
13. Is there emergency lighting in the computer room?				
14. Is there an emergency Power-Off switch located at the exits?				
15. Is there more than one cooling system that will support the computer hardware should one system fail?				
16. Will an alarm sound if the air conditioning system is turned off?				
17. Is the temperature and humidity monitored?				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
18. Will some type of visible or audible alarm sound if the limits are exceeded?				
19. Are fire doors installed at all entrances to the computer room?				
20. Are check forms stored in a secured room?				
21. Are there written instructions for powering up and powering down the system?				
22. Are there written instructions for actions to take in an emergency?				
23. Is there a copy of the DR Plan in the computer room?				
24. Is a procedure library used that contains all the job control necessary to execute job streams?				
25. Is there a formal scheduling system, either computerized or manual?				
26. Is someone assigned to review the schedule and enter all control record information?				
27. Is the entering of control records and similar job control Functions eliminated from operator intervention?				
28. Are tape mounts controlled by a tape- librarian system?				
29. Does an Administrator review reasons why an operator overrides the tape-librarian system?				
30. Does operations management review the console log and error listing to ensure that identifiable errors are corrected and recurring errors are prevented?				
31. Are there written restart procedures for all production systems?				
32. Do the restart procedures indicate that other systems may have to be reprocessed even though they completed successfully?				
33. Do all high priority systems have detail recovery procedures documented?				
34. Are all problems in the computer room documented?				
35. Are metered hours correlated to lapsed time if practical?				
36. Is there a formal Problem Management system, where computer room problems are reviewed by members from operations and programming and remedies assigned?				
37. Is all down time reviewed by operations management?				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
38. Is all production job control reviewed by the operations department after testing is completed and before programs are turned over for production?				
39. Are there Run Manuals for all production applications?				
40. Do the operators have easy access to the Run Manuals?				
41. Are duplicate copies of the Run Manuals stored off site?				
42. Is all special processing for quarterly or annual runs properly documented?				
43. Are batch jobs scheduled for each shift?				
44. Is there a computerized job-accounting system?				
45. Is the job-accounting report reviewed to determine any unusual run patterns?				
46. Are all new systems reviewed for proper file rotation to off-site storage?				
47. Is there a list of all computer hardware including serial numbers, communication equipment and lines, power requirements, cooling requirements, floor space requirements, and acceptable substitute equipment for all the above; and is a copy of this list stored off-site?				
48. Is there a cable layout diagram and plug connector description for the current equipment, and is a copy stored off site?				
49. Is a Provider Information sheet maintained for all Providers supplying computer equipment and supplies?				
50. Have you asked a used hardware Provider for a list of available equipment, in preparation for an emergency?				
51. Are the following backed up daily and rotated off site:				
52. Procedure library?				
53. Tape librarian?				
54. Job scheduling?				
55. Is there a formal procedure for obsolescing a program?				
56. Are the microfiche procedures documented and a copy stored off-site?				
57. Are there any water pipes near or above the computer room?				
58. Is there a threat of water leakage from nearby				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
areas: kitchen, rest rooms, janitor closet, drinking fountain?				
E. TAPE LIBRARY				
1. Is the tape library protected by Halon, FM-200, CO, or sprinklers?				
2. Are smoke detectors located in the tape library?				
3. Does the entrance to the tape library have a fire door?				
4. Does the tape library have emergency lights?				
5. Is access to the tape library restricted by card access or other security?				
6. Is a fire extinguisher mounted outside the door to the tape library?				
7. Has the tape library become a storage area for items other than tapes?				
8. Does the off-site storage for tapes have security, fire protection, 24-hour access, bonded pickup and delivery?				
F. APPLICATION DEVELOPMENT				
1. Is all application software backed up and stored off site?				
2. Do all changes to programs need authorization?				
3. Are there audit trails that identify any program that has been copied for modification, or new program in development?				
4. Is all application software responsible for distributing funds, such as payroll and accounts payable, password protected?				
5. Do the systems above have adequate controls, such as batch totals, hash totals, run totals, and dollar amounts?				
6. Are checks outside the normal range flagged on an audit trail report?				
7. Does an accounts payable audit trail report list the payee for all checks?				
8. Do all financial applications have complete audit trail reports?				
9. Is all of the on-site system documentation stored in fireproof cabinets?				
10. Are users asked to assist in the preparation of test data?				
11. Is there a formal methodology for design and programming?				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
12. Is the design phase completed before the programming phase begins?				
13. Are there written design standards and programming standards?				
14. Are permanent files categorized as critical, important, useful, and non- essential?				
15. Do the standards require the backing up of all critical files?				
16. Are the 3 most current generations of all important and critical files maintained (current, father, grandfather)?				
17. Do the standards require all programs to include proper controls and totals for complete auditing, and for the detection and correction of errors?				
18. Is test data with predetermined results saved and used for heavily maintained systems such as payroll?				
19. Are program changes always made to the source code?				
20. Is the source code maintained on a library that is backed up and rotated off site?				
21. Are the program link-edit reports reviewed for errors and filed with the source code listing?				
22. Are programs always tested even when they have minor modifications?				
23. Does management randomly review program changes and test results?				
24. Do user departments sign off on program modifications and review test results?				
25. Is there a formal procedure for making a program in development a production program?				
26. Are Procedure [Run] Manuals for operations required as part of the program turnover to operations?				
27. Are all modifications to purchased software fully documented and coded in a way that will not disturb the original (provided) source code?				
28. Is a list available of all systems with the person responsible noted?				
29. Is there a list that identifies all programs in a system?				
30. Does each system have a back-up person?				
31. Is documentation kept current?				
32. Is documentation maintained on the computer, backed up, and rotated off site?				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
33. Is there a listing of all technical manuals so they can be replaced if necessary?				
34. Does your company policy state the file retention period for corporation assets information, stockholder information, tax records, employee information, and other vital records?				
35. Are record layouts maintained for the retention period along with the file media?				
36. Has the source information been identified that created the retained data?				
37. Are all databases identified?				
38. Are all programs that update each database identified?				
39. Is the activity that updates the database continually logged?				
40. Are all programs that access each database identified?				
41. Are databases backed up and rotated off site?				
42. Are audit trails available that identify databases that are filling up, and are these reports available on a daily basis?				
43. Are there documented procedures on how to test the validity of each database after it is restored?				
44. Is there documentation that identifies multiple databases that must be kept synchronized with each other?				
G. SYSTEMS & DATABASE SOFTWARE				
1. Is the operating system backed up and rotated off site?				
2. Is a list maintained of all operating system software?				
3. Are the people in the department cross- trained so that everyone has backup?				
4. Are all responsibilities, duties, and procedures documented and a copy stored off site?				
5. Is a Provider Information sheet maintained for all Providers supply ng software?				
6. Have provisions been made for purchased software to execute on another system during an emergency?				
7. Is a copy of the SYSGEN parameters stored off site?				
8. Is there complete documentation explaining how				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
to bring up the operating system at the backup facility?				
9. Is the utilization of all disk devices documented?				
10. Has a plan been formulated on how alternate disk devices would be utilized?				
11. Is there documentation explaining how to modify the JCL to execute at the backup facility?				
H. STATE AUDITOR				
1. Have you reviewed the DR Plan?				
2. Have you observed a recovery test that only used material stored offsite?				
3. Do you periodically review the data center operation and make written recommendations on improvements to procedures, security, and controls?				
4. Are user departments required to balance computer output to manual control totals for audit and security?				
5. Do you save test data to process through cash disbursement systems producing predetermined results?				
I. BACKUP FACILITY				
1. Do you currently subscribe to a fully-equipped backup facility?				
2. Is the backup facility located at a distance that will ensure that an area-wide disaster will not affect the facility?				
3. Is the security at the backup facility at least as good as the security at your current facility?				
4. Have you ever used the backup facility as part of a mock disaster?				
5. Does the backup facility have adequate hours available for testing?				
J. RECIPROCAL AGREEMENTS				
1. Do you have a formal reciprocal agreement currently in effect?				
2. Does the other agency's computer have time available to share with you?				
3. Does your computer have time available to share with another agency?				
4. Are both computer systems compatible?				
5. Do both computer systems have the capacity to				

CHECKLIST QUESTIONS	Yes	No	WIP	ASSIGN/ACTION
process critical applications for both agencies at the same time?				
6. Is the operating system software compatible?				
7. Is there sufficient tape and disk capacity and compatibility?				
8. Will your communication network quickly connect with the other agency's computer?				
9. Does either data center have specialized hardware such as laser printers or cartridge tape drives?				
10. Have both agencies agreed to notify the other about changes in hardware or software?				
11. Will your purchased software execute at the other data center?				
12. Have you tested a critical application at the other data center?				
13. Is there temporary storage available at the other data center for printer forms?				
14. Is there temporary storage available at the other data center for your tape library?				
15. Is there temporary office space available at the other data center for operations support personnel?				

List of Appendices

A. Disaster Recovery Scripts

#	DR Script Filename	Recovery Team Name
	A.1 Network Team	
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
	A.2 Enterprise Systems Team	
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
	A.4 Voice Communications Team	
28		
29		
	A.5 Desktop Team	
30		
31		
32		

A.6 Applications Team

A.7 DR Team

A.8 Operations Team

B. Disaster Recovery Team Checklists

Agency Name

Disaster Recovery Checklist

Once a disaster condition has been declared, the ***(Agency)*** Help Desk will serve as the central point of contact for notifications. This process will start after the Disaster Recovery Coordinator, has notified the appropriate management team to make the declaration official. Following this decision, the ***(Agency)*** Help Desk will begin making the necessary calls to contact everyone in the call chain by priority, using the Emergency Contact list.

B.1 TEAM: Management / Damage Assessment

Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Coordinate initial response using office procedures to protect life and minimize property damage.			
2. Review the disaster site and determine the severity of damages.			
3. Photograph the disaster site if possible.			
4. Prepare report that details damage and outlines disposition of hardware.			
5. Distribute report on damages.			
6. Notify senior management.			
7. Make decisions on implementation of Disaster Recovery Plan.			
8. Notify team captains and start recall process.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
9. Give formal notification (declaration) for request to use backup facilities.			
10. Arrange for emergency funds to cover extra expenses.			
11. If conditions will allow it, establish a Control Center at or near original site and coordinate the recovery. Use the central telephone number or guard's phone as primary contact.			
12. Start Disaster Recovery Logs.			
13. Give senior management scheduled status updates.			
14. Review corporate policy, department budget, and cost-limit guidelines with other teams.			
15. Give users scheduled updates on status through the Help Desk and/or from the Command Center.			
16. Gather Disaster Recovery Logs from all teams. Produce daily status reports.			
17. Arrange for any additional professional help.			
18. Coordinate interviews to fill any vacancies.			
19. Keep status charts of recovery efforts.			
20. Establish transportation to/from backup facilities; arrange scheduled shuttle.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
21. Arrange transportation for materials, people, supplies, and equipment.			
22. Train employees who may be working outside their areas of responsibility.			
23. Administrative services: serve as a clearinghouse for expediting ordering equipment and supplies, making payments, facilitating the process for all team leaders.			
24. Establish internal mail delivery between locations.			
25. Deliver any needed furniture to the backup facility .			
26. Deliver any needed office equipment to the backup facility			
27. Set up any telephones at the backup facility .			
28. Advise other teams of the status of replacement of equipment.			
29. Verify restoration process to ensure integrity and continuity.			
30. Audit financial files to ensure recovery process is complete.			
31. Monitor file restoration, controls, and security during the recovery period.			
32. Give users and Help Desk scheduled updates on status.			

B.2 TEAM: Networks

Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Determine the starting point for network recovery.			
2. Determine damage and requirements to restore communications network.			
3. Identify network needs (bandwidth, ports, IP addressing, etc.).			
4. Identify equipment and order.			
5. Identify data lines and order.			
6. Ensure backup tapes are on site.			
7. Configure network components and data lines.			
8. Test/verify connectivity.			
9. Work with the telephone company to restore full service and place order as needed for replacement telecommunications facilities.			
10. Give Management / Damage Assessment team update on status.			

B.3 TEAM: PC Group

Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Identify DR site requirements.			
2. Identify equipment and order.			
3. Recover configurations, back ups, licenses, etc. from back up storage.			
4. Install applications.			
5. Confirm proper operation.			
6. Configure anti virus server.			
7. Configure LANDesk server.			
8. Give Management / Damage Assessment team update on status.			

B.4 TEAM: Server Group

Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Identify site requirements.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
2. Identify equipment and order.			
3. Recover configurations, back ups, licenses, etc. from backup storage.			
4. Install server software on equipment.			
5. Confirm proper operation.			
6. Confirm network connectivity.			
7. Coordinate with PC group to ensure user's can log on to servers.			
8. Give Management / Damage Assessment team update on status.			

Agency Name
Disaster Recovery Checklist

B.5 TEAM: Operations

Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Assess damage and requirements for necessary replacement equipment.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
2. Establish a Control Center. Give users, Management / Damage Assessment team and Help Desk the phone number of the Control Center.			
3. If hot site available, move operations to hot site until cold site has all necessary equipment for processing (see steps 9 through 12).			
4. Obtain necessary computer equipment for cold site from Providers on the Emergency Provider Contact list.			
5. Notify Provider Field Engineering management to review plan for repair of equipment and installation of delivered units.			
6. Meet with Operations Team members and schedule duties for preparing the backup recovery facilities for any additional equipment.			
7. For backup cold site (shell), review and ensure availability of required power, telephone and communications lines, heating and air-conditioning; work with maintenance personnel to ensure best service from utility companies.			
8. Notify Providers of status and give address of backup facility .			
9. Retrieve needed recovery tapes and documentation for use at backup facility (Hot or Cold).			
10. Assess status of processing and point of recovery for the entire system and/or individual systems. Develop plan to restart operating schedule.			
11. List restart plans for high priority systems and notify all users.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
12. Give Management / Damage Assessment team update on status.			
13. Review list of requirements for supplies.			
14. Arrange for transportation and/or purchase of replacement supplies.			
15. As soon as backup facility is operational, begin to clean up and restore original site.			
16. Check on requirements for cables and connectors and other start-up requirements at the original site.			
17. Schedule testing with maintenance personnel.			
18. Determine the damage to computer equipment and other data center equipment; then work with the Procurement and Administration team to acquire replacements.			

Agency Name
Disaster Recovery Checklist

B.6 TEAM: Applications/Database Software Recovery Team
Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Determine the starting point for application recovery.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
2. Match the latest backup files that Operations plans to use for restoration with user data for reentering.			
3. Obtain original documents to reenter to bring files up to current status.			
4. Determine when equipment will be available.			
5. Arrange for setting up temporary office space.			
6. Notify users of status and inform them on details of restart plan and how to handle input.			
7. Give Management / Damage Assessment team update on status.			
8. Obtain the backup documents and establish revised schedules in conjunction with users and Operations.			
9. Coordinate with Operations and Data Control to verify proper restart point. Verify application software programs and libraries			
10. Restore files and ensure continuity of data by testing and comparing results to users' listings.			
11. Restore databases from backup tapes using recovery documentation.			
12. Restore intermediate data to ensure current integrity.			
13. Perform tests and verify these against user listings.			
14. Process critical applications.			
15. Establish full processing schedule.			

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
16. Ensure continuity by working with users.			
17. Give Management / Damage Assessment team update on status.			

Agency Name
Disaster Recovery Checklist

B.7 TEAM: Systems/Database Software Recovery Team

Date: ____/_____/_____

Team Captain: _____

Alternate: _____

Timed Events	Assigned To	Begin Date Time mm/dd/yy hh:mm	Completed Date Time mm/dd/yy hh:mm
1. Provide the operating systems as well as other control systems software.			
2. Restore the system in priority sequence using backup tapes and verifying continuity.			
3. Work with Provider technical staff as needed.			
4. Notify and inform users of disruptions in services.			
5. Give Management / Damage Assessment team update on status.			

C. (Agency)-DR Test Plan Objectives and Guidelines

A. Test Plan Objectives

Disaster Recovery (DR) plan testing is a critical element of a viable contingency capability. Testing identifies plan deficiencies that need to be addressed. Testing also helps evaluate the ability of the recovery team to implement the plan quickly and effectively. Each DR Test Plan should confirm the accuracy of individual recovery procedures (whether a component test or a full DR test) and the overall effectiveness of the plan(s).

The objectives of DR Plan testing are:
1. To determine if the organization can recover from a variety of scenarios.
2. To ensure that Disaster Recovery Scripts are accurate.
3. To update the Disaster Recovery Plan and/or scripts as needed.
4. To train the DR Team for recovery.
5. To prepare for a disaster situation.

A list of test cases and relevant test procedures are to be documented in the "DR Test Plan". A comprehensive exercise of continuity capabilities and support for designated recovery scripts should be performed on periodic basis.

Addition of new test cases and test case updates are an on going activity and the DR team leader shall ensure the inclusion of required cases. Obsolete cases shall be replaced promptly.

A test auditor must be identified and assigned to observe the execution of DR Test Plans – this person will record all observations. Missing steps/procedures, if any and improvements recommended will be documented in a report. A copy of this report will be provided to DR team leader to ensure updates to the DR Test Plan.

Lessons learned from the results of each DR script execution, test case and inputs from test auditor's report will result in updates to the DR Plan as needed. Updated Disaster Recovery Test Plans will be reviewed for quality.

Document Test Results

The results of the tests conducted for each case are to be documented and signed by the DR team leader.

The results should clearly indicate whether the test has been successful or not. Lessons learned from the test results are to be documented and DR Team must be educated. A knowledge base of lessons learned should be created.

Role of Test Auditor

The test auditors will carryout the following activities:
1. Review the DR Test Plan(s) prior to each DR test.
2. Review the procedures for updating the test plan.

3. Verify that there is effective monitoring of the test plan state of readiness.
4. Ensure that a testing and training schedule exists and is adequate (recommended semi-annually).
5. Observe the test and document all the deviations / shortfalls / inadequacies / exceptions.
6. Develop a report on all observations made during the test and submit it to the DR team leader.
7. Ensure that all weaknesses identified in the most recent exercise have been corrected in an updated version of the test plan.

B. DR Test Plan – Development Guidelines

Disaster recovery plans lay out the steps and strategies to be followed in the event of a technology disaster ... systems failure, network outage or loss of critical data. But these plans lose meaning if they are not tested. Until the disaster happens, disaster plans are largely theoretical ... *what will happen if...*? It is unwise to wait until a disaster is at hand to learn whether your plan is going to work or not. For that reason, it is important to hold regular, realistic tests for your disaster recover plan.

1. Identify Test Objectives

   Disaster recovery planning and related activities require a good deal of effort in terms of financial and staff resources. And while these activities are essential to business survival, they do little to bolster daily workplace productivity. As such, any planning activities should be well thought out, precise and relevant. Along these lines, specific testing plans, intended to verify and validate recovery strategies should be clearly designed with specific goals and purpose in mind. Therefore, as you plan your testing activities, you should carefully consider the following questions….

   - What are the test goals – what is to be accomplished, proven, and/or verified?
   - Are these goals worthwhile in consideration of time, resource constraints, and overall disaster recovery priorities?

2. Identify Test Assumptions

   You should embark upon any testing activities with a set of clearly defined assumptions..... Identifying the defining factors upon which the test is based. These assumptions should accomplish the following:

   - To define the scenario(s) and conditions being tested.
   - To identify test prerequisites (circumstances and/or conditions that must be met for the test to take place).

3. Identify Test Scope

   To keep tests realistic and relevant, it is important to clearly define and limit scope. Test scope sets the parameters for the work to be completed. Test scope should identify the exact systems and/or specific functions to be tested, and it should also

identify any such features or functions that will be excluded. Test scope should be as precise as possible so that all parties are fully aware of the elements being tested. Since it may not be possible to test every element or scenario, it is also important to establish test limitations up front. As you prepare your scope, you should consider the following questions…

- What systems and functions will your test include?
- What systems and functions are excluded?
- Why are those systems and functions being excluded?

4. Establish Success Criteria

   How will you know if your test is a success? While success can be simply defined as "does our recovery plan work, and did our systems perform as expected?" ... actual success can be far more diverse. It is possible that your test plan may succeed simply by proving systems weaknesses or disaster recovery planning failures. In this case, your test was a success because it served its purpose. In any event, identified success criteria are an important part of any test plan, to avoid potential confusion and false expectations regarding test objectives and results. Along these lines, there are two primary aspects to these success criteria....

   - **Plan Success**: did the test plan accomplish its goal - i.e. have you learned what you thought you would?

   - **Technical Success**: did the systems or functions tested meet technical recovery goals?

   Whatever your specific success criteria may be, these various criteria will be your launching pad for action once the test is completed. When you are able to compare test results to defined success criteria, you will be able to form a clear road to action, whether you need to make technical changes, management changes, procedural changes, or planning changes.

5. Clarify Roles & Responsibilities

   In order to conduct effective, efficient tests, it is important to clearly establish roles and responsibilities for all groups and individuals involved. This specification of roles and responsibilities should accomplish the following:

   - To identify the individuals, business units and service providers involved in the test, as well as their various roles and responsibilities

   - To define the roles and responsibilities necessary to execute the test plan, including test specifics, test participation, results review, approvals and recommendations.

6. Identify Logistical Requirements (Schedules, Premises & Equipment)

   In order to execute meaningful disaster recovery tests, you will need to identify and specify logistical requirements. These requirements provide the physical means for the test – how it is conducted, where it is conducted, and what tools are needed. Test logistics include specific schedules, physical premises, and physical tools (hardware, software and supplies).

   The specification of these logistical requirements should include a schedule for all test activities, as well as a list of all physical test requirements - which can include premises, hardware, software, supplies, late hours meals or transportation, and security access.

7. Clarify Business Impact

   While disaster events can have a serious, disruptive impact on business operations, any activities to test disaster plans can also be disruptive, albeit on a very limited and temporary basis. When you test your recovery plans, these tests will probably involve production systems, perhaps rendering any such systems inaccessible for test period. Most of us would not choose to conduct these tests in the middle of the work week, but considering the **"24 x 7"** nature of business technology, there may very well be no good time to conduct testing activities. Therefore, you should look to schedule tests for minimal disruption, but when that is not possible, you will need to communicate operational consequences to test participants and your end user community.

   When considering the disruptive nature of disaster recovery tests, you will need to address the following questions:

   - Will production systems be involved, and will there be any downtime during the test?
   - Are there any risks involved in the actual testing process?
   - When will normal operations resume?

8. Provide Test Scripts

   To ensure test success and consistency, disaster recovery test plans should include test scripts, detailing the actions and activities required to actually conduct the technical elements of the test. Depending upon the nature of the test, these scripts can be simple or complex, and can be used to provide instructions to test participants.

9. Specify Test Activities

   In order to properly plan any disaster recovery test, you will need to describe and specify the activities involved in preparing, conducting and reviewing the test. At the time that a test is conducted, it should be as efficient and effective as possible. To achieve that goal, tests should be broken down into smaller, manageable components, listing specific tasks and activities required to prepare for, execute, and react to test results.

- What do you need to do to prepare for the test?
- What activities are required to execute the test activities?
- What will happen once the test is completed?
- How will results be recorded and analyzed for lessons learned and potential corrective actions?

10. Obtain the Necessary Approvals

    To solidify management support, internal visibility, and acceptance of overall results, it is important to ensure that your disaster test plans follow structured procedures for approval and acceptance. This serves several key goals….

    - To ensure that all parties agree to the goals, objectives, scope and specific tasks involved in the actual test process.
    - To ensure that all parties accept and agree to assigned roles and responsibilities – establishing ownership in the testing process and the results.
    - To ensure that all parties are informed, particularly with relationship to test dates and potential impact on production systems.
    - To ensure that test results are properly analyzed, verified and put in proper perspective for remedial action.

11. Post- Test Activities

    This section should describe post-test activities ... i.e. What will happen once the test is completed? How will results be recorded and analyzed for lessons learned and potential corrective actions?

12. Test Plan Approvals

    This section should provide for the signatures of any individuals who must accept and authorize the test plan.

D. (Agency)-DR GO Box

D.1 Go Box Contents

i. A Go Box is used to store backup copies of media (tapes, CDs, DVDs, etc.) and procedural documentation (including recovery scripts), as well as other equipment needed to restore applications and data to an operational state.
There should be separate Excel workbooks containing an inventory of each Go Box for each of the following groups:

(1) Applications
(2) Networks
(3) Servers
(4) Desktops
(5) Voice
(6) Admin-Management