IT Disaster Recovery Plan Template

By CherryRoad Technologies Inc.

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0			

An information technology (IT) disaster recovery (DR) plan provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure, which includes hardware, software, networks, processes, and people. Protecting your firm's investment in its technology infrastructure and protecting your firm's ability to conduct business are the key reasons for implementing an IT disaster recovery plan.

Table of Contents

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency, modifications to this document may be made to ensure physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan.
- The need to ensure that operational policies are adhered to within all planned activities.
- The need to ensure that proposed contingency arrangements are cost-effective.

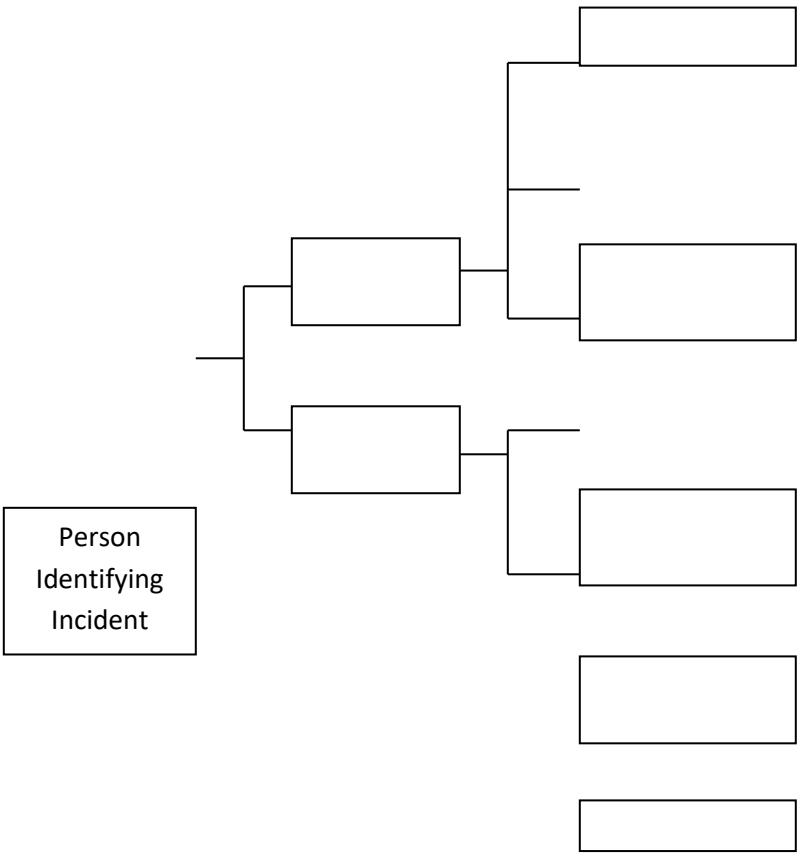
- The need to consider implications on other company sites.
- Disaster recovery capabilities as applicable to key customers, vendors, and others.

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

Name, Title	Contact Option	Contact Number
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

Notification Calling Tree



External Contacts

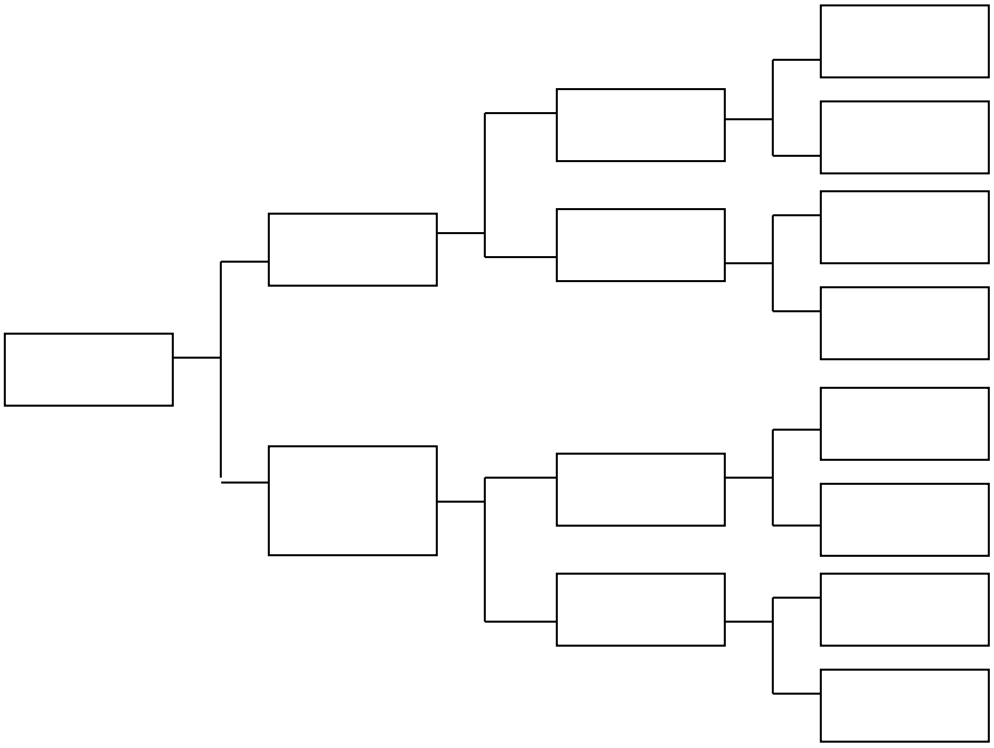
Name, Title	Contact Option	Contact Number
Landlord / Property Manager		
Account Number None		
	Work	
	Mobile	
	Home	
	Email Address	
Power Company		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Telecom Carrier 1		
Account Number	Work	
	Mobile	
	Fax	
	Home	
	Email Address	
Telecom Carrier 2		
Account Number	Work	
	Mobile	

Name, Title	Contact Option	Contact Number
	Home	
	Email Address	
Hardware Supplier 1		
Account Number	Work	
	Mobile	
	Emergency Reporting	
	Email Address	
Server Supplier 1		
Account Number.	Work	
	Mobile	
	Fax	
	Email Address	
Workstation Supplier 1		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Office Supplies 1		
Account Number C3095783	Work	
	Mobile	
	Home	

Name, Title	Contact Option	Contact Number
	Email Address	
Insurance – Name		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Site Security –		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Off-Site Storage 1		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Off-Site Storage 2		
Account Number	User ID	
	Password	
	Home	
	Email Address	

Name, Title	Contact Option	Contact Number
HVAC –		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Power Generator –		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
Other –		
Account Number	Work	
	Mobile	
	Home	
	Email Address	

External Contacts Calling Tree



1 Plan Overview

1.1 Plan Updating

It is necessary for the DRP updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the IT Director.

1.2 Plan Documentation Storage

Copies of this Plan, CD, and hard copies will be stored in secure locations to be defined by the company. Each member of senior management will be issued a CD and hard copy of this plan to be filed at home. Each member of the Disaster Recovery Team and the Business Recovery Team will be issued a CD and hard copy of this plan. A master protected copy will be stored on specific resources established for this purpose.

1.3 Backup Strategy

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at the company's offices in _____. This strategy entails the maintenance of a fully mirrored duplicate site which will enable instantaneous switching between the live site (headquarters) and the backup site.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Purchasing	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Warehouse & Inventory	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site

Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site
Web Site	Fully mirrored recovery site

1.4 Risk Management

There are many potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Probability: 1=Very High, 5=Very Low Impact: 1=Total destruction, 5=Minor annoyance

Potential Disaster	Probability Rating	Impact Rating	Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience

2 Emergency Response

2.1 Alert, escalation, and plan invocation

2.1.1 Plan Triggering Events

Key trigger issues at headquarters that would lead to activation of the DRP are:

- Total loss of all communications
- Total loss of power
- Flooding of the premises
- Loss of the building

2.1.2 Assembly Points

Where the premises need to be evacuated, the DRP invocation plan identifies two evacuation assembly points:

- Primary – Far end of main parking lot
- Alternate – Parking lot of company across the street

2.1.3 Activation of Emergency Response Team

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster and call emergency services.
- Assess the extent of the disaster and its impact on the business, data center, etc.
- Decide which elements of the DR Plan should be activated.
- Establish and manage disaster recovery team to maintain vital services and return to normal operation.
- Ensure employees are notified and allocate responsibilities and activities as required.

2.2 Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 2.0 business hours;
- Restore key services within 4.0 business hours of the incident;
- Recover to business as usual within 8.0 to 24.0 hours after the incident;
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team.

2.3 Emergency Alert, Escalation and DRP Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the company returns to normal operating mode.

2.3.1 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

Emergency Response Team

- _____
- _____
- _____

If not available try:

- _____
- _____

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan, as well as in the event of any other occurrence that affects the company's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The Business Recovery Team (BRT) will consist of senior representatives from the main business departments. The BRT Leader will be a senior member of the company's management team and will be responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

2.3.2 DR Procedures for Management

Members of the management team will keep a hard copy of the names and contact numbers of each employee in their departments. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans on file in their homes if the headquarters building is inaccessible, unusable, or destroyed.

2.3.3 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot

reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

2.3.4 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

2.3.5 Recorded Messages / Updates

For the latest information on the disaster and the organization's response, staff members can call a toll-free hotline listed in the DRP wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

2.3.7 Alternate Recovery Facilities / Hot Site

If necessary, the hot site at SunGard will be activated and notification will be given via recorded messages or through communications with managers. Hot site staffing will consist of members of the disaster recovery team only for the first 24 hours, with other staff members joining at the hot site as necessary.

2.3.8 Personnel and Family Notification

If the incident has resulted in a situation which would cause concern to an employee's immediate family such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

3 Media

3.1 Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

3.2 Media Strategies

1. Avoiding adverse publicity
2. Take advantage of opportunities for useful publicity
3. Have answers to the following basic questions:
    - What happened?
    - How did it happen?
    - What are you going to do about it?

3.3 Media Team

- _____
- _____
- _____

3.4 Rules for Dealing with Media

Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

4 Insurance

As part of the company's disaster recovery and business continuity strategies several insurance policies have been put in place. These include errors and omissions, directors & officers' liability, general liability, and business interruption insurance.

If insurance-related assistance is required following an emergency out of normal business hours, please contact: _____

Policy Name	Coverage Type	Coverage Period	Amount of Coverage	Person Responsible For Coverage	Next Renewal Date

5 Financial and Legal Issues

5.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of check books, credit cards, etc.
- Loss of cash

5.2 Financial Requirements

The immediate financial needs of the company must be addressed. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, Social Security, etc.
- Availability of company credit cards to pay for supplies and services required post-disaster

5.3 Legal Actions

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc.

6 DRP Exercising.

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

Appendix A – Technology Disaster Recovery Plan Templates

Disaster Recovery Plan for <System One>

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER	Provide details
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details

Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM ONE ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Data	Provide details
Scenario 2 Total Loss of HW	Provide details

ADDENDUM

CONTACTS	

File Systems <date>

File System as of <date> Minimal file systems to be created and restored from backup: <List>	**Filesystem** **kbytes** **Used** **Avail** **%used** **Mounted on** <Provide details>
Other critical files to modify	<Provide details>
Necessary directories to create	<Provide details>
Critical files to restore	<Provide details>
Secondary files to restore	<Provide details>
Other files to restore	<Provide details>

Disaster Recovery Plan for <System Two>

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER	Provide details
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details

Offsite Storage	Provide details

BACKUP STRATEGY for SYSTEM TWO	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM TWO ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Data	Provide details
Scenario 2 Total Loss of HW	Provide details

ADDENDUM

CONTACTS	

File Systems <date>

File System as of <date> Minimal file systems to be created and restored from backup: <List>	**Filesystem** **kbytes** **Used** **Avail** **%used** **Mounted on** <Provide details>
Other critical files to modify	<Provide details>
Necessary directories to create	<Provide details>
Critical files to restore	<Provide details>
Secondary files to restore	<Provide details>
Other files to restore	<Provide details>

Disaster Recovery Plan for Local Area Network (LAN)

SYSTEM	

OVERVIEW	
SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER	Provide details
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details

Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

BACKUP STRATEGY for SYSTEM TWO	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM TWO ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Data	Provide details
Scenario 2 Total Loss of HW	Provide details

ADDENDUM

CONTACTS	

File Systems <date>

File System as of <date> Minimal file systems to be created and restored from backup: <List>	**Filesystem** **kbytes** **Used** **Avail** **%used** **Mounted on** <Provide details>
Other critical files to modify	<Provide details>
Necessary directories to create	<Provide details>
Critical files to restore	<Provide details>
Secondary files to restore	<Provide details>
Other files to restore	<Provide details>

Disaster Recovery Plan for Wide Area Network (WAN)

SYSTEM	

OVERVIEW	
EQUIPMENT	Location: Device Type: Model No.: Technical Specifications: Network Interfaces: Power Requirements; System Serial #: DNS Entry: IP Address: Other:
HOT SITE EQUIPMENT	Provide details
SPECIAL APPLICATIONS	
ASSOCIATED DEVICES	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details

Offsite Storage	Provide details
Network Services	Provide details

BACKUP STRATEGY for SYSTEM TWO	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM TWO ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Network	Provide details
Scenario 2 Total Loss of HW	Provide details

ADDENDUM

CONTACTS	

Support Systems <date>

Support system	<Provide details>
Critical network assets	<Provide details>
Critical interfaces	<Provide details>
Critical files to restore	<Provide details>
Critical network services to restore	<Provide details>
Other services	<Provide details>

Disaster Recovery Plan for Remote Connectivity

SYSTEM	

OVERVIEW	
EQUIPMENT	Location: Device Type: Model No.: Technical Specifications: Network Interfaces: Power Requirements; System Serial #: DNS Entry: IP Address: Other:
HOT SITE EQUIPMENT	Provide details
SPECIAL APPLICATIONS	
ASSOCIATED DEVICES	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

Network Services	Provide details

BACKUP STRATEGY for SYSTEM TWO	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM TWO ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Network	Provide details
Scenario 2 Total Loss of HW	Provide details

ADDENDUM

CONTACTS	

Support Systems <date>

Support system	<Provide details>
Critical network assets	<Provide details>
Critical interfaces	<Provide details>
Critical files to restore	<Provide details>
Critical network services to restore	<Provide details>
Other services	<Provide details>

Disaster Recovery Plan for Voice Communications

SYSTEM	

OVERVIEW	
EQUIPMENT	Location: Device Type: Model No.: Technical Specifications: Network Interfaces: Power Requirements; System Serial #: DNS Entry: IP Address: Other:
HOT SITE EQUIPMENT	Provide details
SPECIAL APPLICATIONS	
ASSOCIATED DEVICES	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

Network Services	Provide details

BACKUP STRATEGY for SYSTEM TWO	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM TWO ***DISASTER RECOVERY PROCEDURE***	
Scenario 1 Total Loss of Switch	Provide details
Scenario 2 Total Loss of Network	Provide details

ADDENDUM

CONTACTS	

Support Systems <date>

Support system	<Provide details>
Critical network assets	<Provide details>
Critical interfaces	<Provide details>
Critical files to restore	<Provide details>
Critical network services to restore	<Provide details>
Other services	<Provide details>

Appendix B – Suggested Forms

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

_____

Management of DR Activities Form

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughout the disaster recovery period;
- All actions that occur during this phase will need to be recorded.

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	Completion Date/Time	Resources Involved	In Charge

Disaster Recovery Event Recording Form

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:
Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	Date and Time	Outcome	Follow-On Action Required

Disaster Recovery Team's Work Completed: <Date>
Event Log Passed to Business Recovery Team: <Date>

_____

Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management.

The report will include:

- A description of the emergency or incident.
- Those people notified of the emergency (including dates).
- Action taken by members of the DRT.
- Outcomes arising from actions taken.
- An assessment of the impact to normal business operations.
- Assessment of the effectiveness of the BCP and lessons learned.
- Lessons learned.

_____

Mobilizing the Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed on standby.
- The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed.

Description of Emergency:
Date Occurred:
Date Work of Disaster Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

_____

Mobilizing the Business Recovery Team Form

- Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.
- The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

Description of Emergency:
Date Occurred:
Date Work of Business Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period.
- Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated.

Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.

Recovery Tasks (*Order of Priority)*	Person(s) Responsible	Completion Date		Milestones Identified	Other Relevant Information
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					
7.					

Preparing the Business Recovery Report Form

- On completion of business recovery activities, the BRT leader should prepare a report on the activities undertaken and completed.
- The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be distributed to senior management, as appropriate.

The contents of the report shall include:

- A description of the incident.
- People notified of the emergency (including dates).
- Action taken by the business recovery team.
- Outcomes arising from actions taken.
- An assessment of the impact to normal business operations.
- Problems identified.
- Suggestions for enhancing the disaster recovery and/or business continuity plan.
- Lessons learned.

Communications Form

- It is very important during the disaster recovery and business recovery activities that all affected persons and organizations are kept properly informed.
- The information given to all parties must be accurate and timely.
- Any estimate of the timing to return to normal working operations should be announced with care.
- It is also very important that only authorized personnel deal with media queries.

Groups of Persons or Organizations Affected by Disruption	Persons Selected To Coordinate Communications to Affected Persons / Organizations		
	Name	Position	Contact Details
Customers			
Management & Staff			
Suppliers			
Media			
Stakeholders			
Others			

_____

Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader.
- This process should be formalized to ensure that all parties understand the change in overall responsibility, and the transition to business-as-usual.
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead.
- It is assumed that business unit management will be fully involved throughout the recovery, but for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team.

_____

Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management *(If different than completion date)*	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: _____

Signature: _____

Date: _____

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions.

Name: _____

Title: _____

Signature: _____

Date: _____

Creating a service level agreement (SLA) is one of the most critical steps to aligning your business's IT operations with an MSP's capabilities.

Traditionally, an SLA defines exactly what a client will receive from a service provider. These agreements are crucial to building trust and ensuring satisfaction for both parties.

Service Level Agreement: The Basics

A service level agreement serves three primary functions:

1. Expectation setting: Detailing client and MSP responsibilities
2. Rule setting: Identifying the consequences if expectations aren't met. This will include conditions of cancellation.
3. Scorecard creation: Goal setting and performance requirements.

The SLA is a set of rules that help the client and MSP set goals and create agreements so both parties can be as successful as possible.

DRaaS SLA for Business Continuity Planning

A DRaaS SLA should reflect the requirements set out in the business continuity plan, especially those legally binding regulatory requirements.

Disaster Recovery as a Service (DRaas) solutions are designed to provide peace of mind. When disaster strikes, a business needs to know that their data is safe in the cloud. An SLA outlining the terms and conditions of recovery requirements ensures that all data recovery expectations will be met. If they are not, the consequences are evident.

A carefully negotiated SLA can reduce frustration and dissatisfaction, and support a healthy, productive business relationship. The SLA will address:

- Business continuity requirements
- Downtime
- Scalability
- Elasticity
- Data location
- Security

SLAs to Support Data Security

A service level agreement written to address security can help to minimize data leakage and theft. Many DRaaS SLAs include encryption keys and certifications to prevent security breaches and unauthorized data access. In the case of a security, compliance or privacy breach, the SLA promises prompt notification – and the ability to respond quickly and efficiently.

Supporting Business Growth

As your business changes and grows, so too should your DRaaS SLA. Changing strategic, operational, and technical requirements should be reflected in Disaster Recovery planning and the SLA. That means the SLA must be treated as a living document and be reviewed periodically to ensure it reflects the realities of the business.

As a business grows, the allocated resources may not be able to respond to larger requirements. As a client, you must alert your MSP to your changing needs. The MSP will need to adapt resources so systems can be restored in the required period. For a DRaaS solution to be successful and robust, transparency between both parties is key.

Service Level Agreement Effectiveness

An SLA protects the interests of both the client and the Managed Service Provider.

By setting expectations in an SLA, the client and the MSP know exactly what to expect for post-disaster recovery. Both parties can rest assured knowing what steps must be taken to meet recovery time and recovery point objectives.

With this level of transparency, an MSP offering DRaaS can provide peace of mind that your business will never be without service.

At HopOne, we take data protection and site operation seriously. In the unfortunate case of disaster, our disaster recovery services retrieve and restore your data instantly from the cloud. Our service achieves bare metal recovery within minutes, ensuring

uninterrupted service. Learn more about our DRaaS and our approach to SLAs via your account representative.

What are the main challenges associated with DRaaS SLAs, and how should cloud providers approach them?

The terms for a Disaster Recovery as a (DRaaS) service-level agreement (SLA) need to be carefully reviewed and negotiated upfront by the cloud provider and customer, followed by the customer paying for the appropriate SLA required. It is a good idea to discuss a potential SLA with all the stakeholders in the business, along with a lawyer specializing in IT SLAs to ensure that all areas and challenges are addressed properly. The time spent preparing an SLA is well worthwhile and will greatly reduce future problems, frustration, and dissatisfaction.

A well-thought-out SLA should address several challenges associated with information transfer to and from the cloud. It should also touch upon mobility, availability, business continuity, scalability, and elasticity. In addition, regarding physical location information, it is important for providers to disclose in an SLA where the data will be stored. The reason for this is that cloud providers may federate with other providers to provide elasticity, and this could result in noncompliance or a privacy breach, making it even more important to have full disclosure.

Being up front about data validation and ensuring data integrity in the cloud always is also key. Customers also value immediate verification of backup, replicated data and disaster recovery (DR), along with a solid guarantee of information recovery and business continuity.

Replicas of all protected systems should be frequently updated by incremental backups or snapshots. These should be scheduled by the user for each system according to recovery point objectives. Regarding these snapshots, customers must be able to monitor who will be granted access to them for security reasons. Similarly, it is critical for security reasons to set a standard for when snapshots are allowed, where they are stored and for how long they are stored by the provider's system administrators.

It is also important for SLAs to include full site, system, disk and file recovery services that are completely user-driven, self-service portals to allow the user the flexibility of choice as to what system or file disk they want to recover. The ability to converge backup and replication silos into one homogeneous system that supports both disk and tape is also a differentiator. Backup is all about recovery, and customers will not compromise in that area when choosing a cloud service for backup and DR.

Security is another differentiating factor. Security policies that are consistent with the security policies of a customer's organization are ideal. One way to accomplish this is by making sure temporary files and data are deleted upon completion of the task being performed. This strategy, along with the snapshot security measures, will minimize data leakage and theft. Put procedures in place for preventing security breaches and

unauthorized data access, including careful storage of encryption keys and certifications. In addition, if there is a security, compliance or privacy breach, there should be prompt notification and communication of the situation to the customer.

An effective SLA should also address the anticipated restoration time should there be a disaster. A reasonable response time in which files and system disks should be restored is within 30 minutes. Be sure to conduct both scheduled and unscheduled DR rehearsals and tests that demonstrate to customers the viability of your DR plan to ensure that it can be carried out as planned.

Transparency is also important in the sense that it is a good idea for the DRaaS provider to notify the business of any new risk, security or any incidences that may affect the customer adversely.

For Disaster Recovery as a Service (DRaaS)

Contact: Tim Sexton

Email: info@cherryroad.com /sales@hopone.net

Tel. 571.282.6321 / Cell 571.426.9824