

# **CONTROL YOUR DESTINY: A DISASTER RECOVERY PLANNING TEMPLATE FOR YOUR BUSINESS**

**A FILL-ABLE PDF FORM DESIGNED FOR  
IT PROS AND BUSINESS EXECUTIVES**



**First**  
Communications®



**Executive Brief**

## 1. OVERVIEW

- 1.1 Introduction
- 1.2 Purpose
- 1.3 Priorities

## 2. UNDERSTAND YOUR BUSINESS

- 2.1 About your business
  - 2.1.1 Business description
  - 2.1.2 Current IT environment
  - 2.1.3 Current network services descriptions
  - 2.1.4 Define critical business processes
- 2.2 Risk assessment scorecard

## 3. DR PREPARATIONS AND RISK MITIGATION

- 3.1 Disaster recovery and business continuity
  - 3.1.1 Goals
  - 3.1.2 Define objectives
  - 3.1.3 Checklist
  - 3.1.4 Gaps
  
- 3.2 Establish teams
  - 3.2.1 Key business stakeholders
  - 3.2.2 Disaster recovery team
  - 3.2.3 Calling tree
  - 3.2.4 Outside vendors
  
- 3.3 Key areas of preparation
  - 3.3.1 Call center
  - 3.3.2 Emergency messages
  - 3.3.3 Passwords, product keys, warranty info
  - 3.3.4 Network connectivity
  - 3.3.5 Backups
  - 3.3.6 Inventory of systems
  - 3.3.7 Remote workers (Hot Sites)
  - 3.3.8 Redundancy/High availability

## 4. RECOVERY PLAN

- 4.1 Declare emergency
- 4.2 Mobilize DR team
- 4.3 Notify employees
- 4.4 Restoration process
  - 4.4.1 Restore critical processes for emergency level of service
  - 4.4.2 Restore processes for key business services
  - 4.4.3 Restore to business as usual
- 4.5 Scenarios
  - 4.5.1 Loss of power (Example Scenario 1)
  - 4.5.2 IT systems failure (Example Scenario 2)

- 4.5.3 Loss of access to building (Example Scenario 3)
- 4.5.4 Create more scenarios

## **5 FOLLOW UP AND REPORTING TEMPLATE**

- 5.1 Damage and assessment
- 5.2 Insurance
- 5.3 Financial impact / BIA
- 5.4 Recovery success evaluation
- 5.5 Suggest improvement to plan

## **6 OVERALL PLAN MANAGEMENT**

- 6.1 Distribution
- 6.1 Repository
- 6.3 Accessibility
- 6.4 Change management
- 6.5 Alternate versions

## **7 DRILL AND PRACTICE.**

## **APPENDIX**

- Appendix A- Systems Inventory

# 1. OVERVIEW

## 1.1 INTRODUCTION

This document is a comprehensive disaster recovery plan prepared documenting the key systems and resources that must be recovered in the case of an IT systems failure.

Do not restrict yourself to the version of this document, which Cloudnition has provided. This template is a starting point; as disaster recovery plans naturally evolve with time, you are encouraged to make changes to the template to best fit your business. Add sections that fall outside the scope of Cloudnition's expertise and remove sections that do not apply to your business.

## 1.2 PURPOSE

The purpose of this exercise is to provide a structured methodology and framework for a disaster recovery plan that will allow the user to continue and recover critical business processes in the event of a disaster that compromised IT systems.

This document will be used to assess and mitigate your current level of risk, develop a disaster recovery team, gather and organize critical contact information, gather and organize critical systems information, identify and prioritize key business practices, set disaster recovery objectives, create an executable recovery plan, and report and track recovery in the event of a disaster.

## 1.3 PRIORITIES

This document will assist in defining the critical priorities for continuing or restoring your business operations whether it be customer communications, website functionality, storefront on main street, or whatever your specific business needs are. This document will also prioritize IT systems essential to critical business processes. Based on these critical priorities and the business continuity solutions in place, this document will also assist in creating disaster recovery objectives.

# 2. UNDERSTAND YOUR BUSINESS

## 2.1 ABOUT YOUR BUSINESS

### 2.1.1 BUSINESS DESCRIPTION

A short business description that should include industry, number of employees, organization chart, list of departments, etc.

### 2.1.2 CURRENT IT ENVIRONMENT

What is your current technology infrastructure comprised of?

### 2.1.3 CURRENT NETWORK SERVICES DESCRIPTION

Include: Upload/download speed, number of internet connections, number of providers, type of network, backup providers, description of provided services.



### 3.1.1 GOALS

What are your goals for disaster recovery? Is there a business process that should be uninterrupted during disaster?

### 3.1.2 DEFINE RECOVERY OBJECTIVES

Set goals for your recovery which are specific to your businesses needs as well as its capabilities.

**Recovery Level Objective (RLO):** Prioritize your recovery, after disaster strikes it is unlikely that you can recover everything instantly and simultaneously. What do you need for emergency level of service? What do you need to launch key business processes? What do you need for business as usual? Will your objectives be categorized into more than three groups?

**Recovery Time Objective (RTO):** For each level of recovery provide a recovery time objective. Be aware of what your capabilities are, granular recovery of important emails is much faster than recovering entire exchange servers.

Level of Recovery	Recovery Time Objective
Establish an emergency level of service within	
Restore Key Services within	
Recover to BAU within	

### Recovery Point Objective (RPO):

The recovery point objective is the point back in time to which you wish to restore from. This will be your most recent backup. For example if you want to restore data to the way it looked an hour before the disaster then you should be backing up every hour. The way you set your RPO will dictate how often you should perform backups. Your Recovery Point Objective could be different for each file system; those, which are mission critical, should be backed up continuously or very often. Less important, or non-mission critical, files can be backed up less frequently.

### 3.1.3 CHECKLIST

What technologies do you currently have in place to aid in the disaster recovery process? Are there any you want to add? Any you are curious about?

Business Continuity Process	Yes	No	I want that	What is that?
<b>Local Backups</b>				
<b>Cloud Backups</b>				
<b>Call Rerouting Capabilities</b>				
<b>Fully Redundant Hot Site</b>				
<b>Uninterrupted Power Supply</b>				
<b>Backup generator</b>				
<b>4G wireless internet connection</b>				

### 3.1.4 GAPS

Is there any solution you need to implement to reach the objectives set in 3.1.2

## 3.2 ESTABLISH TEAMS

### DISASTER RECOVERY TEAMS

Your disaster recovery team should be fully capable of restoring your key business processes after a disaster. The disaster recovery process should be overseen by key business stakeholders. The stakeholders are typically c-level members of the organization who have a stake in their department. The disaster recovery team should be comprised of members from each department of your company and should be fully capable.

#### 3.2.1 KEY BUSINESS STAKEHOLDERS - DEPT HEADS

The key business stakeholders are usually department heads, c-level executives, and principals. These people may have a financial interest in recovering quickly. At most mid sized and large organizations these people will not directly contribute to the recovery process; however, at small and very small businesses these people will likely be an integral part of both the key business stakeholders and the disaster recovery team.

Name, Title	Contact Option	Contact Number
<b>IT Systems</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
<b>Financial</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
<b>Sales</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
<b>HR</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
<b>Marketing</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

### 3.2.2 DISASTER RECOVERY TEAM

Disaster Recovery Coordinators are the most important people on the day of a disaster. Usually these are IT managers, operations managers, and financial managers. They have the capabilities to restart and reconfigure systems, resume key business processes, open communications, and make critical financial decisions. After selecting coordinators, the rest of the team should be filled with other employees capable of helping the coordinators execute the disaster recovery plan.

Name, Title	Contact Option	Contact Number
<b>DR Coordinator</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
<b>DR Coordinator 2</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

### 3.2.2 ALTERNATE DISASTER RECOVERY TEAM MEMBERS

Always have backups!

Name, Title	Contact Option	Contact Number
<b>Alternate Coordinator</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
<b>Alternate Coordinator 2</b>	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	
	Work	
	Alternate	
	Mobile	
	Home	
	Email Address	
	Alternate Email	

### 3.2.3 CALLING TREE

Cloudnition suggests building a call tree, we also suggest having this calling tree in section 4.2 of this document.

### 3.2.4 OUTSIDE VENDORS

Keep a list of important outside contact information. The following list has been filled in, feel free to customize it for your organization. (examples)

Name, Title	Contact Option	Contact Number
<b>Landlord / Property Manager</b>		
Account Number None		
	Work	
	Mobile	
	Home	
	Email Address	
<b>Power Company</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Telecom Carrier 1</b>		
Account Number	Work	
	Mobile	
	Fax	
	Home	
	Email Address	
<b>Telecom Carrier 2</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Hardware Supplier 1</b>		
Account Number	Work	
	Mobile	
	Emergency Reporting	
	Email Address	
<b>Server Supplier 1</b>		
Account Number.	Work	
	Mobile	
	Fax	
	Email Address	
<b>Workstation Supplier 1</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Office Supplies 1</b>		
Account Number C3095783	Work	
	Mobile	
	Home	
	Email Address	

Name, Title	Contact Option	Contact Number
<b>Insurance – Name</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Site Security –</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Off-Site Storage 1</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Cloud Storage</b>		
Account Number	User ID	
	Password	
	Home	
	Email Address	
<b>HVAC –</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Power Generator –</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	
<b>Other –</b>		
Account Number	Work	
	Mobile	
	Home	
	Email Address	

### 3.3 KEY AREAS OF PREPARATION

#### 3.3.1 CALL CENTER

Usually communication is number one priority for a company. Do you have a call center that you need to relocate after a disaster, or can you reroute calls to an alternate call center. How do you plan on fielding calls?

#### 3.3.2 EMERGENCY OUTGOING MESSAGES (VOICEMAIL, E-MAIL, SMS, SOCIAL MEDIA)

Do you have the ability to disperse outgoing messages to your employees and contacts? What medium of communication do they use? How do you initiate the messages?

#### 3.3.3 ESSENTIAL PASSWORDS, PRODUCT KEYS, AND WARRANTY INFORMATION

You can report non-private passwords here or password locations; otherwise, password owners can be identified with contact info provided. Critical and private passwords should be kept offsite in a safe or safety deposit box.

##### Passwords

System	Username/Login	Password/Password Owner

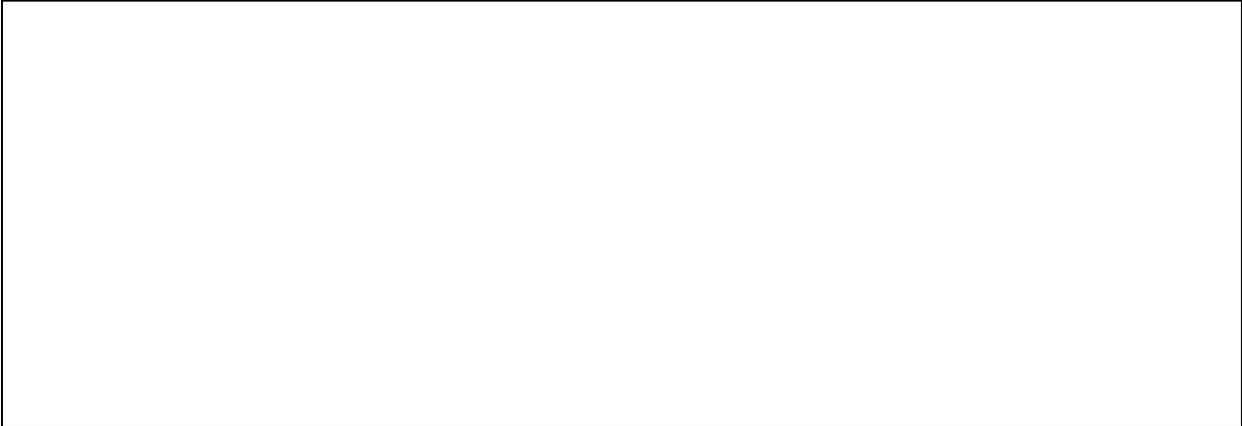
##### Program License Keys

Program	License Key	Other



### 3.3.6 KNOW YOUR HARDWARE [REFER TO APPENDIX A]-

It is important to know what hardware you are currently running your systems on. This information could be critical if you need to replace some of your hardware. You must identify and record technical specifications, physical locations, model numbers, disk size, vendors, applications, warranty information, and other critical information.



### 3.3.7 REMOTE WORKERS (HOT SITES)

Prepare and designate alternate/remote work sites

In the event that the office is inaccessible, it is a good strategy to have an alternate site, or a location where you can temporarily resume emergency or key business processes until a permanent location is secured. This may be another branch office, a stand by emergency office, the nearest Starbucks, or a work from home arrangement.

#### 3.3.7A COLD SITE

A cold site is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

**-OR-**

#### 3.3.7B HOT SITE

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site

exists so that the organization can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less.

### 3.3.8 REDUNDANCY AND HIGH AVAILABILITY OPTIONS

#### EXAMPLE 1 – FULLY MIRRORED HOT SITE

Key business processes and the agreed backup strategy for each are listed below. The strategy chosen is for a fully mirrored recovery site at \_\_\_\_\_. 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	REDUNDANT CLONE or HIGH AVAILABILITY STRATEGY
IT Operations	
Tech Support - Hardware	
Tech Support - Software	
Development/Engineering	
QA	
Monitoring	
Facilities Management	
Email	
Purchasing	
Disaster Recovery	
Finance	
Contracts Admin	
Warehouse & Inventory	
Product Sales	
Business Development	
Human Resources	

#### EXAMPLE 2 – HIGH AVAILABILITY VIRTUALIZATION AND HYBRID CLOUD

## 4. RECOVERY PLAN

### 4.1 DECLARE EMERGENCY

Person identifying disaster should immediately contact the DR Leaders. Define any other protocols you may find necessary for this person after indentifying a disaster.

### 4.2 MOBILIZE DR TEAM – CALLING TREE

How will you mobilize your Disaster Recovery Team? Calling trees are usually your best option. Don't forget cell phone numbers and alternates coordinators. Other methods include e-mail, collaboration tools, SMS tools, etc.

### 4.3 NOTIFY EMPLOYEES

Once the disaster recovery team gets to work, how will you notify the rest of your employees. What instructions would you likely give them.

## 4.4 RESTORE PROCESS

Document the order in which to restore processes.

### 4.4.1 RESTORE CRITICAL PROCESSES FOR EMERGENCY LEVEL OF SERVICE

Decide beforehand which business processes are required to provide an emergency level of service to your customer. You can find some of this information from section 2.1.4. What is absolutely essential to you making money or keeping customers from leaving? What dependencies do those processes have? And what steps must be taken to recover said processes?

Rank	Business Process	Dependencies	Other Instructions

### 4.4.2 RESTORE PROCESSES FOR KEY BUSINESSES SERVICES

Rank	Business Process	Dependencies	Other Instructions

### 4.4.3 RESTORE PROCESSES FOR BUSINESS AS USUAL

Rank	Business Process	Dependencies	Other Instructions

### 4.5 SCENARIOS

Choose some scenarios and create predesigned responses for them. Identify where you are most vulnerable. What will you experience often and what will hurt you most?

[Snow Storms, Robbery, Fire, Gas Leak, Flood, Flu Outbreak]

#### 4.5.1 LOSS OF POWER TO BUILDING


#### 4.5.2 IT SYSTEMS FAILURE


#### 4.5.3 BUILDING EVACUATION




### 5.3 FINANCIAL/BIA

Use this section to assess financial impacts the disaster has on your business

Financial Impact	Description	Exact/Estimated Cost
Lost sales		
Lost customers		
Compliance/Regulatory		
Reputation damage		
Hardware damage		
Productivity		
Physical Damage		

### 5.4 RECOVERY SUCCESS EVALUATION

Create a list of everything that had to be recovered, whether the recovery was successful, and how long it took.

System	Success/Fail	Time to Recovery (actual/objective)

### 5.5 SUGGESTED IMPROVEMENT TO DR PLAN

Fill out suggestions on how to improve this plan after disasters and drills.

## 6. OVERALL PLAN MANAGEMENT

### 6.1 DISTRIBUTION

Each employee should have a hard copy both at home and the office.

## 6.2 REPOSITORY

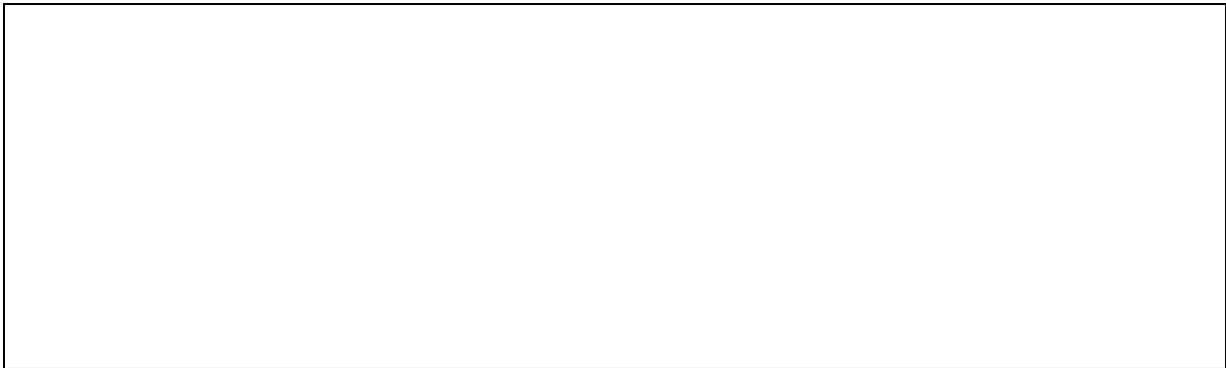
An electronic version should be distributed which should be stored onsite and backed up to the cloud for remote access.

## 6.3 ACCESSIBILITY

We also suggest publishing an online .pdf form on your website or employee portal.

## 6.4 CHANGE MANAGEMENT

Some of the information in this document will change over time. This is an IT DR plan so we suggest that your disaster recovery coordinator who is in the IT department be responsible for that aspect. This person is likely most familiar with the plan and on the disaster day he/she is the one who will depend on this plan. Document new hardware, software, service providers, and personnel.



## 6.5 ALTERNATE VERSIONS

This disaster recovery plan may hold sensitive information. Will each employee have the same version? Employees with different responsibilities or clearance levels may receive different versions of this plan.

## 7. DRILL AND PRACTICE

Schedule regular drills, every 6 months or more often. Run drills as if they are real disasters and always make upgrades and modifications to improve the disaster recovery documents. This should be a living-breathing document that evolves with your business to provide the best possible outcome from unexpected IT disasters. **Next Scheduled DR Drill:**



## Appendix – Systems Inventory

### 3.3.6 Inventory of Systems – APPENDIX

#### SERVERS

<i>SYSTEM</i>	
---------------	--

<i>OVERVIEW</i>	
<b>PRODUCTION SERVER</b>	Location: Server Model: Operating System: CPUs: Memory: Total Disk: % Used: System/Admin Handle: System/Admin Password: System Serial #: DNS Entry: IP Address: Other: Warranty Information:
<b>HOT SITE SERVER</b>	Provide details if applicable
<b>APPLICATIONS</b> (Use bold for Hot Site)	
<b>ASSOCIATED SERVERS</b>	

<i>KEY CONTACTS</i>	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	
Offsite Storage	

<i>BACKUP STRATEGY FOR SYSTEM ONE</i>	
<b>Daily</b>	
<b>Weekly</b>	
<b>Monthly</b>	

<b>SERVER ONE</b> <b>DISASTER RECOVERY PROCEDURE</b>	
Scenario 1 Total Loss of Data	Provide details
Scenario 2 Total Loss of HW	Provide details

**ADDENDUM - Internal contact information for help troubleshooting server solutions**

<b>CONTACTS</b>	

**File Systems <date>**

File System as of <date>	Filesystem	kbytes	Used	Avail	%used	Mounted on
Minimal file systems to be created and restored from backup: <List>	<Provide details> Critical file directories must be restored first, depending on how much data you have full restoration could be too long to wait for some of your files. Based on estimated speed to recovery (5mbs for online restore) prioritize files to be restored, small files can be restored in less than a second, large folders could take hours, plan accordingly.					
Other critical files to modify						
Necessary directories to create						
Critical files to restore						
Secondary files to restore						
Other files to restore						

## Local Area Network

<i>SYSTEM</i>	
---------------	--

<i>OVERVIEW</i>	
<b>Firewall</b>	Internet Service Provider: Account information: Device Type: Model Number: Technical Specifications: Power Requirements: System Serial #: DNS Entry: IP Address: VPN: Port Settings: Other:
<b>HOT SITE EQUIPMENT</b>	
<b>SPECIAL APPLICATIONS</b>	
<b>ASSOCIATED SERVERS</b>	
<b>KEY CONTACTS</b>	
<b>Hardware Vendor</b>	
<b>System Owners</b>	

<i>OVERVIEW</i>	
<b>Modem</b>	Internet Service Provider: Internet Type: Account information: Device Type: Model Number: Technical Specifications: Power Requirements: System Serial #: DNS Entry: IP Address: Other:
<b>HOT SITE EQUIPMENT</b>	
<b>SPECIAL APPLICATIONS</b>	
<b>ASSOCIATED SERVERS</b>	
<b>KEY CONTACTS</b>	
<b>Hardware Vendor</b>	
<b>System Owners</b>	

<i>OVERVIEW</i>	
<b>Router</b>	Device Type: Model Number: Technical Specifications: Power Requirements: System Serial #: DNS Entry: IP Address: Routing Protocols: Passwords/Security Type: Wi-fi Security Protocol: Other:
<b>HOT SITE EQUIPMENT</b>	
<b>SPECIAL APPLICATIONS</b>	
<b>ASSOCIATED SERVERS</b>	
<b>KEY CONTACTS</b>	
<b>Hardware Vendor</b>	
<b>System Owners</b>	

<i>OVERVIEW</i>	
<b>Switch</b>	Device Type: Model Number: Technical Specifications: Power Requirements: System Serial #: DNS Entry: IP Address: Routing Settings: Other:
<b>HOT SITE EQUIPMENT</b>	
<b>SPECIAL APPLICATIONS</b>	
<b>ASSOCIATED SERVERS</b>	
<b>KEY CONTACTS</b>	
<b>Hardware Vendor</b>	
<b>System Owners</b>	

<i>BACKUP STRATEGY for SYSTEM TWO</i>	<b>You can backup your running configurations. Firewall settings, switch configurations, router configurations, etc</b>
<i>Daily</i>	
<i>Monthly</i>	
<i>Quarterly</i>	

<b>SYSTEM TWO</b> <b>DISASTER RECOVERY</b> <b>PROCEDURE</b>	
Scenario 1 Stops Working	Provide details
Scenario 2 Damage/Loss of HW	Provide details

**ADDENDUM**

<b>CONTACTS</b>	

Systems Inventory for Voice Communications

<b>SYSTEM</b>	
---------------	--

<i>OVERVIEW</i>	
<b>EQUIPMENT</b>	Location: Provider: Phone Type: <b>PBX, VoIP</b> Manufacturer: Model No.: Technical Specifications: Mac Address Network Interfaces: Power Requirements; System Serial #: DNS Entry: IP Address: Other: <b>Local Lines, 800 numbers, PRI SIP POTS, tel #s, fax#s, alarms, private lines, point to point lines, personal lines</b>
<b>HOT SITE EQUIPMENT</b>	<b>Provide details</b>
<b>SPECIAL APPLICATIONS</b>	
<b>ASSOCIATED DEVICES</b>	

<i>KEY CONTACTS</i>	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	
Offsite Storage	
Network Services Provider	

<i>BACKUP STRATEGY for SYSTEM TWO</i>	
<b>Daily</b>	
<b>Monthly</b>	
<b>Quarterly</b>	

<b>SYSTEM TWO</b> <b>DISASTER RECOVERY</b> <b>PROCEDURE</b>	
Scenario 1 Loss of Network	Provide details
Scenario 2 Loss of Hardware	Provide details

**ADDENDUM**

<b>CONTACTS</b>	

**Support Systems <date>**

Support system	
Critical network assets	
Critical interfaces	
Critical files to restore	
Critical network services to restore	
Other services	