

# IT Disaster Recovery Plan Template

BY PAUL KIRVAN, CISA, FBCI

#### 32 page Disaster Recovery template, including:

- ✓ Directions on how to create a DR plan and understand objectives
  - ✓ Steps to take through the early phase of the incident
    - ✓ Tips for dealing with the media
  - ✓ Actions to take when facing financial and legal issues

# **Revision History**

| REVISION     | DATE | NAME | DESCRIPTION |
|--------------|------|------|-------------|
| Original 1.0 |      |      |             |
|              |      |      |             |
|              |      |      |             |

# **Table of Contents**

| Information Technology Statement of Intent                          |    |
|---|----|
| Policy Statement  |    |
| Objectives  | 3  |
| Key Personnel Contact Info  | 4  |
| Notification Calling Tree   | 5  |
| External Contacts   | 6  |
| External Contacts Calling Tree                                      | 9  |
| 1 Plan Overview   | 10 |
| 1.1 Updates   | 10 |
| 1.2 Documentation Storage   | 10 |
| 1.3 Backup Strategy   | 10 |
| 1.4 Risk Management   | 10 |
| 2 Emergency Response  | 12 |
| 2.1 Alert, Escalation and Plan Invocation                           | 12 |
| 2.2 Disaster Recovery Team  |    |
| 2.3 Emergency Alert, Escalation and DRP Activation                  | 12 |
| 3 Media   |    |
| 3.1 Media Contact   |    |
| 3.2 Media Strategies  |    |
| 3.3 Media Team  |    |
| 3.4 Rules for Dealing with Media                                    |    |
| 4 Insurance   |    |
| 5 Financial and Legal Issues  | 16 |
| 5.1 Financial Assessment  |    |
| 5.2 Financial Requirements  |    |
| 5.3 Legal Actions   |    |
| 6 DRP Exercising  |    |
| Appendix A – Technology Disaster Recovery Plan Templates            |    |
| Disaster Recovery Plan for <system one=""></system>                 |    |
| Disaster Recovery Plan for <system two=""></system>                 |    |
| Disaster Recovery Plan for Local Area Network (LAN)                 |    |
| Disaster Recovery Plan for Wide Area Network (WAN)                  |    |
| Disaster Recovery Plan for Remote Connectivity                      |    |
| Disaster Recovery Plan for Voice Communications                     |    |
| Appendix B – Suggested Forms  |    |
| Damage Assessment Form  | 31 |
| Management of DR Activities Form                                    |    |
| Disaster Recovery Event Recording Form                              |    |
| Disaster Recovery Activity Report Form                              |    |
| Mobilizing the Disaster Recovery Team Form                          |    |
| Mobilizing the Business Recovery Team Form                          |    |
| Monitoring Business Recovery Task Progress Form                     |    |
| Preparing the Business Recovery Report Form                         |    |
| Communications Form   |    |
| Returning Recovered Business Operations to Business Unit Leadership |    |
| Business Process/Function Recovery Completion Form                  | 35 |

# 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 situation, modifications to this document may be made to ensure the physical safety of our people, our systems, and our data.

Our mission is to ensure information system uptime, data integrity and availability, local/remote access to information systems and services, 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 account for changing circumstances.

# **Objectives**

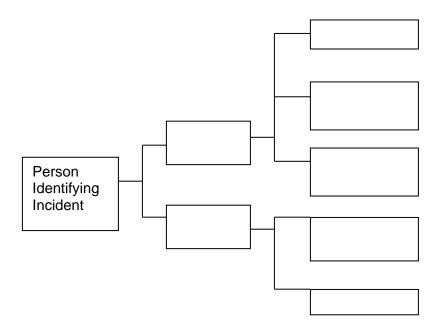
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan that will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency that interrupts information systems and business operations.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

- all employees must fully understand their duties in implementing the plan;
- operational policies are adhered to within all planned activities;
- the proposed contingency arrangements are cost-effective, and management must consider implications on other company sites.

# **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 |                |
|             |                 |                |
|             | 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**



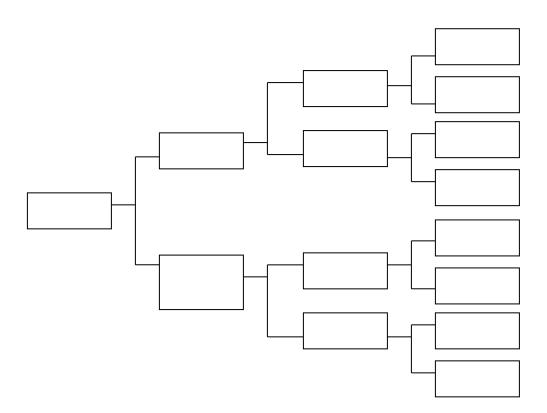
# **External Contacts**

| Name, Title                        | Contact Option                    | Contact Number |
|------------------------------------|-----------------------------------|----------------|
| Landlord / Property                | Contact Option                    | Contact Number |
| Manager                            |                                   |                |
| Account Number                     | Work                              |                |
|                                    | Mobile                            |                |
|                                    | Emergency Reporting               |                |
|                                    | Email Address                     |                |
|                                    |                                   |                |
| Power Company                      |                                   |                |
| Account Number                     | Work                              |                |
|                                    | Mobile                            |                |
|                                    | Emergency Reporting               |                |
|                                    | Email Address                     |                |
|                                    |                                   |                |
| Telecom Carrier 1                  |                                   |                |
| Account Number                     | Work                              |                |
|                                    | Mobile                            |                |
|                                    | Emergency Reporting               |                |
|                                    | Email Address                     |                |
|                                    |                                   |                |
| Telecom Carrier 2                  |                                   |                |
| Account Number                     | Work                              |                |
|                                    | Mobile                            |                |
|                                    | Emergency Reporting               |                |
|                                    | Email Address                     |                |
|                                    |                                   |                |
| Cloud Service Provider 1           |                                   |                |
| Account Number                     | Work                              |                |
|                                    | Mobile                            |                |
|                                    | Emergency Reporting               |                |
|                                    | Email Address                     |                |
| Outron and the Drawit day 4        |                                   |                |
| Cybersecurity Provider 1           | Monte                             |                |
| Account Number                     | Work<br>Mobile                    |                |
|                                    |                                   |                |
|                                    | Emergency Reporting Email Address |                |
|                                    | Email Address                     |                |
| Hardware Supplier 1                |                                   |                |
| Hardware Supplier 1 Account Number | Work                              |                |
| ACCOUNT NUMBER                     | Mobile                            |                |
|                                    |                                   |                |
|                                    | Emergency Reporting Email Address |                |
|                                    | LIIIAII AUUIESS                   |                |
| Disaster Recovery Supplier         |                                   |                |
| 1                                  |                                   |                |
| Account Number                     | Work                              |                |
|                                    | Mobile                            |                |
|                                    | Emergency Reporting               |                |
|                                    | Email Address                     |                |
|                                    |                                   |                |
| ·                                  |                                   |                |

| Name, Title                              | Contact Option      | Contact Number |
|--|---------------------|----------------|
|  |                     |                |
| Server Supplier 1                        |                     |                |
| Account Number.                          | Work                |                |
|  | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
| M. I. ( 0 1; 4                           |                     |                |
| Workstation Supplier 1                   | )                   |                |
| Account Number                           | Work                |                |
|  | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
| Office Supplies 1                        |                     |                |
| Office Supplies 1 Account Number         | Work                |                |
| Account Number                           | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
|  | Email Address       |                |
| Insurance                                |                     |                |
| Account Number                           | Work                |                |
| Account Number                           | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
|  | Linaii Addiess      |                |
| Site Security                            |                     |                |
| Account Number                           | Work                |                |
| 7 10 0 0 0 11 11 1 1 1 1 1 1 1 1 1 1 1 1 | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
|  |                     |                |
| Off-Site Storage 1                       |                     |                |
| Account Number                           | Work                |                |
|  | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
|  |                     |                |
| Off-Site Storage 2                       |                     |                |
| Account Number                           | Work                |                |
|  | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
|  |                     |                |
| HVAC                                     | 1207                |                |
| Account Number                           | Work                |                |
|  | Mobile              |                |
|  | Emergency Reporting |                |
|  | Email Address       |                |
| Pookup Dower Concrete                    |                     |                |
| Backup Power Generator Account Number    | Mork                |                |
| Account Number                           | Work<br>Mobile      |                |
|  |                     |                |
|  | Emergency Reporting |                |

| Name, Title                | Contact Option      | Contact Number |
|----------------------------|---------------------|----------------|
| Name, me                   | Email Address       | Contact Number |
|                            | Email Address       |                |
| Local Hospital             |                     |                |
| Account Number             | Work                |                |
| Account Number             | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            | Liliali Addiess     |                |
| Company Physician          |                     |                |
| Account Number             | Work                |                |
| Account I variber          | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            | Email / tadioco     |                |
| Mental Health Professional |                     |                |
| Account Number             | Work                |                |
| , toodant running.         | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            | Zman / tagrees      |                |
| Medical Supplies           |                     |                |
| Account Number             | Work                |                |
|                            | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            |                     |                |
| Alternate Office Space 1   |                     |                |
| Account Number             | Work                |                |
|                            | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            |                     |                |
| Alternate Office Space 2   |                     |                |
| Account Number             | Work                |                |
|                            | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            |                     |                |
| Other                      |                     |                |
|                            | Work                |                |
|                            | Mobile              |                |
|                            | Emergency Reporting |                |
|                            | Email Address       |                |
|                            |                     |                |

# **External Contacts Calling Tree**



# 1 Plan Overview

#### 1.1 Updates

It is necessary for the disaster recovery plan updating process to be properly structured and controlled. Whenever changes are made to the plan they must 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 Documentation Storage

Digital and hard copies of this plan will be stored in secure locations to be defined by the company. Each member of senior management will be issued a digital 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 digital 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. The location of this site will be either at a company location or at a remotely hosted location, such as a cloud service provider or managed services provider.

| KEY BUSINESS PROCESS                 | BACKUP STRATEGY                             |
|--------------------------------------|---|
| IT Operations                        | Fully mirrored recovery site; cloud service |
| Tech Support - Hardware and Software | Fully mirrored recovery site; cloud service |
| Remote Working                       | Fully mirrored recovery site; cloud service |
| Cybersecurity Management             | Fully mirrored recovery site; cloud service |
| Physical Security                    | Fully mirrored recovery site; cloud service |
| Email                                | Fully mirrored recovery site; cloud service |
| Purchasing                           | Fully mirrored recovery site; cloud service |
| Disaster Recovery                    | Fully mirrored recovery site; cloud service |
| Data Backup Storage                  | Fully mirrored recovery site; cloud service |
| Systems Backup                       | Fully mirrored recovery site; cloud service |
| Finance                              | Fully mirrored recovery site; cloud service |
| Contracts Administration             | Fully mirrored recovery site; cloud service |
| Warehouse & Inventory                | Fully mirrored recovery site; cloud service |
| Product Sales                        | Fully mirrored recovery site; cloud service |
| Maintenance Sales                    | Fully mirrored recovery site; cloud service |
| Human Resources                      | Fully mirrored recovery site; cloud service |
| Alternate Work Areas                 | Fully mirrored recovery site; cloud service |
| Call/Contact Center                  | Fully mirrored recovery site; cloud service |
| Website                              | Fully mirrored recovery site; cloud service |
|                                      |   |

#### 1.4 Risk Management

There are many potential disruptive threats that can occur at any time and affect normal business processes. 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 situation 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:

| Potential Disaster                      | Probability<br>Rating | Impact<br>Rating | Brief Description Of Potential Consequences & Remedial Actions   |
|---|-----------------------|------------------|--|
| Flood                                   | 3                     | 3                | All critical equipment is located on 1st Floor; remote work  |
| Fire                                    | 3                     | 2                | FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors; remote work   |
| Tornado                                 | 5                     | 2                | Loss of building; remote work; secure new location   |
| Electrical storms                       | 5                     | 2                | Loss of power; remote work   |
| Act of terrorism                        | 5                     | 3                | Damage to building and resources; remote work  |
| Act of sabotage                         | 5                     | 3                | Damage to building and resources; remote work  |
| Electrical power failure                | 3                     | 2                | Redundant uninterruptible power supply (UPS) array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored; remote work |
| Loss of communications network services | 4                     | 2                | Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience; remote work  |

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

# 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 DR plan are:

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

#### 2.1.2 Assembly Points

Where the premises need to be evacuated, the 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 DR plan 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 and data center;
- determine if an evacuation is needed;
- decide which elements of the DR plan should be activated;
- establish and manage disaster recovery team to maintain vital services and return to normal operations,
   and
- ensure employees are notified and allocate responsibilities and activities as required.

#### 2.2 Disaster Recovery Team

The disaster recovery team will be contacted and assembled by the ERT. This team's responsibilities are to:

- establish facilities for an emergency level of service within two business hours;
- activate access to IT services for remote working within two hours;
- restore key services within four business hours of the incident;
- recover to business as usual within 8-24 hours after the incident;
- coordinate activities with disaster recovery team and first responders, and
- 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

When using emergency alert systems, the person discovering the incident will call a member of the Emergency Response Team in the order listed:

| Er        | mergency   | Response | Team |
|-----------|------------|----------|------|
| • -       |            | _        |      |
| • -       |            | _        |      |
| • -       |            | _        |      |
| lf<br>• _ | not availa | ble try: |      |
|           |            | _        |      |

The emergency response team is responsible for activating the DR plan 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 that an emergency has occurred. The notification will request disaster recovery team members to assemble at the site of the problem and will involve sufficient information to have this request effectively communicated. The business recovery team will consist of senior representatives from the main business departments. The business recovery team 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 in the event that the headquarters building is inaccessible, unusable, or destroyed. Management should be prepared to order employees to work remotely.

#### 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. Employees should be prepared to work remotely if assigned.

#### 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 provided to each employee. This may be provided to them through email, text message or a hard copy wallet card. Included in messages will be data on the nature of the disaster, assembly sites, and updates on work resumption.

#### 2.3.6 Alternate Recovery Facilities / Hot Sites

If necessary, an emergency IT recovery facility 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. If a cloud recovery facility has been arranged, it will be activated and placed into service to ensure all mission-critical systems, applications and data are available.

#### 2.3.7 Personnel and Family Notification

If the incident has resulted in a situation that 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. If employees are ordered to go home and work remotely, they should notify family members of that change as soon as possible.

# 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 communications during and after the event.

#### 3.2 Media Strategies

- 1. Avoid 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 electronic and print media; anyone else contacted should refer callers or in-person media representatives to the media team. Plans for social media use should be developed and distributed to all employees.

### 4 Insurance

As part of the company's disaster recovery and business continuity strategies, a number of 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<br>Type | Coverage<br>Period | Amount Of<br>Coverage | Person<br>Responsible<br>For Coverage | Next<br>Renewal<br>Date |
|-------------|------------------|--------------------|-----------------------|---------------------------------------|-------------------------|
|             |                  |                    |                       |                                       |                         |
|             |                  |                    |                       |                                       |                         |
|             |                  |                    |                       |                                       | _                       |

# 5 Financial and Legal Issues

#### 5.1 Financial Assessment

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

- 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
- Availability of company credit cards to pay for supplies and services required post-disaster

#### 5.3 Legal Actions

The company legal department and emergency response team will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event, such as the possibility of claims by or against the company for regulatory violations.

# 6 DRP Exercising

Disaster recovery plan exercises, especially if remote working by employees is indicated, are an essential part of the plan development process. Plan exercises ensure that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities, and that the technologies are available and operational.

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>** 

| Disaster | recovery | iaii ioi | <b>Coystelli</b> | OII |
|----------|----------|----------|------------------|-----|
| SYSTEM   |          |          |                  |     |

| OVERVIEW                      |                         |
|-------------------------------|-------------------------|
| PRODUCTION SI                 | ERVER Location:         |
|                               | Server Model:           |
|                               | Operating System:       |
|                               | CPUs:                   |
|                               | Memory:                 |
|                               | Total Disk:             |
|                               | System Handle:          |
|                               | System Serial #:        |
|                               | DNS Entry:              |
|                               | IP Address:             |
|                               | Other:                  |
| HOT SITE SI                   | ERVER Provide details   |
| CLOUD SITE SI                 | ERVER   Provide details |
| APPLICA                       | ATIONS                  |
| (Use bold for Hot/Cloud Site) |                         |
| ASSOCIATED SER                | RVERS                   |

| KEY CONTACTS          |                 |
|-----------------------|-----------------|
| Hardware Vendor       | Provide details |
| System Owners         | Provide details |
| Database Owner        | Provide details |
| Application Owners    | Provide details |
| Software Vendors      | Provide details |
| Cloud Service Vendors | Provide details |
| Offsite Storage       | Provide details |

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

| SYSTEM ONE<br>DISASTER RECOVERY<br>PROCEDURE |                 |
|--|-----------------|
| Scenario 1                                   | Provide details |
| Total Loss of Data                           |                 |
| Scenario 2                                   | Provide details |
| Total Loss of Hardware                       |                 |

#### ADDENDUM

| CONTACTS |  |
|----------|--|
|          |  |
|          |  |
|          |  |
|          |  |

# File Systems <date>

| File System as of <date></date>                              | Filesystem kby                 | tes Used | Avail | %used | Mounted on |
|--|--------------------------------|----------|-------|-------|------------|
| Minimal file systems to be created and restored from backup: | <provide details=""></provide> |          |       |       |            |
| <list></list>  |                                |          |       |       |            |
|  |                                |          |       |       |            |
| Other critical files to modify                               | <provide details=""></provide> |          |       |       |            |
| Necessary directories to create                              | <provide details=""></provide> |          |       |       |            |
| Critical files to restore                                    | <provide details=""></provide> |          |       |       |            |
| Secondary files to   | <provide details=""></provide> |          |       |       |            |
| restore  |                                |          |       |       |            |
| Other files to restore                                       | <provide details=""></provide> |          | -     |       |            |
| Primary data backup  | <provide details=""></provide> |          | -     |       |            |
| Alternate data backup  | <provide details=""></provide> |          |       |       |            |

# Disaster Recovery Plan for <System Two>

| OVERVIEW                |                   |
|-------------------------|-------------------|
| PRODUCTION              | Location:         |
| SERVER                  | Server Model:     |
|                         | Operating System: |
|                         | CPUs:             |
|                         | Memory:           |
|                         | Total Disk:       |
|                         | System Handle:    |
|                         | System Serial #:  |
|                         | DNS Entry:        |
|                         | IP Address:       |
|                         | Other:            |
| HOT SITE SERVER         | Provide details   |
| CLOUD SITE SERVER       | Provide details   |
| APPLICATIONS            |                   |
| (Use bold for Cloud/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 |
| Cloud Service Vendors | Provide details |
| Offsite Storage       | Provide details |

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

| SYSTEM TWO<br>DISASTER RECOVERY<br>PROCEDURE |                 |
|--|-----------------|
| Scenario 1                                   | Provide details |
| Total Loss of Data                           |                 |
| Scenario 2                                   | Provide details |
| Total Loss of HW                             |                 |

| CONTACTS |  |
|----------|--|
|          |  |
|          |  |
|          |  |
|          |  |

# File Systems <date>

| File System as of <date>  Minimal file systems to be created and restored from</date> | Filesystem <provide deta<="" th=""><th>kbytes<br/>ails&gt;</th><th>Used</th><th>Avail</th><th>% used</th><th>Mounted on</th></provide> | kbytes<br>ails> | Used | Avail | % used | Mounted on |
|---|--|-----------------|------|-------|--------|------------|
| backup:   |  |                 |      |       |        |            |
| <list></list>   |  |                 |      |       |        |            |
|   |  |                 |      |       |        |            |
| Other critical files to modify  | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |
| Necessary directories to create   | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |
| Critical files to restore   | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |
| Secondary files to restore  | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |
| Other files to  | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |
| restore Primary data backup   | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |
| Alternate data backup   | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide>  | ails>           |      |       |        |            |

# **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:            |
| CLOUD SITE SERVICE  | Provide details   |
| APPLICATIONS        |                   |
| (Use bold for Cloud |                   |
| Service)            |                   |
| ASSOCIATED SERVERS  |                   |

| KEY CONTACTS          |                 |
|-----------------------|-----------------|
| Hardware Vendor       | Provide details |
| System Owners         | Provide details |
| Database Owner        | Provide details |
| Application Owners    | Provide details |
| Software Vendors      | Provide details |
| Cloud Service Vendors | Provide details |
| Offsite Storage       | Provide details |

| BACKUP STRATEGY for LANS |                 |
|--------------------------|-----------------|
| Daily                    | Provide details |
| Monthly                  | Provide details |
| Quarterly                | Provide details |

| LANS DISASTER<br>RECOVERY<br>PROCEDURE |                 |
|--|-----------------|
| Scenario 1                             | Provide details |
| Total Loss of LAN1                     |                 |
| Scenario 2                             | Provide details |
| Total Loss of LAN2                     |                 |

| CONTACTS |  |
|----------|--|
|          |  |
|          |  |
|          |  |
|          |  |

# File Systems <date>

| File System as of <date></date>                              | Filesystem  | kbytes | Used | Avail | %used | Mounted on |
|--|---|--------|------|-------|-------|------------|
| Minimal file systems to be created and restored from backup: | VI Tovide det   | alis>  |      |       |       |            |
| Other critical files to modify                               | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |
| Necessary directories to create                              | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |
| Critical files to restore                                    | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |
| Secondary files to restore                                   | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |
| Other files to restore                                       | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |
| Primary data backup  | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |
| Alternate data backup  | <provide deta<="" td=""><td>ails&gt;</td><td></td><td></td><td></td><td></td></provide> | ails>  |      |       |       |            |

# **Disaster Recovery Plan for Wide Area Network (WAN)**

#### NETWORK

| 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           |
| MANAGED SERVICE PROVIDER EQUIPMENT | Provide details           |
| CLOUD EQUIPMENT                    | Provide details           |
| SPECIAL SERVICES                   |                           |
| SPECIALIZED 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<br>DISASTER RECOVERY<br>PROCEDURE |                 |
|--|-----------------|
| Scenario 1                                   | Provide details |
| Total Loss of WAN                            |                 |
| Scenario 2                                   | Provide details |
| Total Loss of WAN<br>Hardware                |                 |

| CONTACTS |  |
|----------|--|
|          |  |
|          |  |
|          |  |
|          |  |

# Support Systems <date>

| Support system          | <provide details=""></provide> |
|-------------------------|--------------------------------|
| Critical network assets | <provide details=""></provide> |
| Critical interfaces     | <provide details=""></provide> |
| Critical files to       | <provide details=""></provide> |
| restore                 |                                |
| Critical network        | <provide details=""></provide> |
| services to restore     |                                |
| Cloud network           | <provide details=""></provide> |
| services                |                                |
| Other services          | <provide details=""></provide> |

# **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:                    |
| CLOUD SERVICES   | Provide details           |
| SPECIAL SERVICES | Provide details           |
| MOBILE DEVICES   | Provide details           |

| KEY CONTACTS           |                 |
|------------------------|-----------------|
| Remote Software Vendor | Provide details |
| Workstation/Laptop     | Provide details |
| Vendors                |                 |
| Remote Application     | Provide details |
| Owners                 |                 |
| Remote Software        | Provide details |
| Vendors                |                 |
| Cloud Services         | Provide details |
| Network Services       | Provide details |

| BACKUP STRATEGY for REMOTE ACCESS |                 |
|-----------------------------------|-----------------|
| Daily                             | Provide details |
| Monthly                           | Provide details |
| Quarterly                         | Provide details |

| REMOTE ACCESS<br>DISASTER RECOVERY<br>PROCEDURE |                 |
|---|-----------------|
| Scenario 1                                      | Provide details |
| Total Loss of Internet                          |                 |
| Scenario 2                                      | Provide details |
| Total Failure of Remote<br>Access Services      |                 |

| CONTACTS |  |
|----------|--|
|          |  |
|          |  |
|          |  |
|          |  |

# **Support Systems <date>**

| Remote systems      | <provide details=""></provide> |
|---------------------|--------------------------------|
| Internet access     | <provide details=""></provide> |
| Critical interfaces | <provide details=""></provide> |
| Remote software     | <provide details=""></provide> |
| Other network       | <provide details=""></provide> |
| services to restore |                                |
| Cloud services      | <provide details=""></provide> |
| Other services      | <provide details=""></provide> |

# **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:                    |
| CLOUD EQUIPMENT      | Provide details           |
| SPECIAL APPLICATIONS | Provide details           |
| MOBILE DEVICES       | Provide details           |

| 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 |
| Cloud Voice Services | Provide details |

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

| SYSTEM TWO<br>DISASTER RECOVERY<br>PROCEDURE |                 |
|--|-----------------|
| Scenario 1                                   | Provide details |
| Total Loss of Switch                         |                 |
| Scenario 2                                   | Provide details |
| Total Loss of Network                        |                 |

| CONTACTS |  |
|----------|--|
|          |  |
|          |  |
|          |  |
|          |  |

# **Support Systems <date>**

| Voice system        | <provide details=""></provide> |
|---------------------|--------------------------------|
| Critical network    | <provide details=""></provide> |
| assets              | D 11 1 ( 11                    |
| Critical interfaces | <provide details=""></provide> |
| Critical files to   | <provide details=""></provide> |
| restore             |                                |
| Critical network    | <provide details=""></provide> |
| services to restore |                                |
| Cloud voice         | <provide details=""></provide> |
| services            |                                |
| Other services      | <provide details=""></provide> |

# **Appendix B – Suggested Forms**

#### **Damage Assessment Form**

| <b>Description Of Problem</b> | Extent Of Damage       |
|-------------------------------|------------------------|
|                               |                        |
|                               |                        |
|                               |                        |
|                               |                        |
|                               |                        |
|                               |                        |
|                               |                        |
|                               | Description Of Problem |

#### **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<br>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<br>Required |
|----------------------------------|---------------|---------|------------------------------|
|                                  |               |         |                              |
|                                  |               |         |                              |
|                                  |               |         |                              |
|                                  |               |         |                              |
|                                  |               |         |                              |
|                                  |               |         |                              |
|                                  |               |         |                              |

| Disaster Recovery Team's Work Completed: <date></date>    |
|---|
| Event Log Passed to Business Recovery Team: <date></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 the following:

- · A description of the emergency or incident
- People notified of the emergency
- Dates people were notified
- Action taken by members of the disaster recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the business continuity plan 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<br>Team<br>Member                      | Contact<br>Details | Contacted<br>On (Time /<br>Date) | By Whom | Response | Start Date<br>Required |
|--|--------------------|----------------------------------|---------|----------|------------------------|
|  |                    |                                  |         |          |                        |
|  |                    |                                  |         |          |                        |
|  |                    |                                  |         |          |                        |
|  |                    |                                  |         |          |                        |
| Relevant Comments/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<br>Team<br>Member                      | Contact<br>Details | Contacted<br>On (Time /<br>Date) | By Whom | Response | Start Date<br>Required |
|--|--------------------|----------------------------------|---------|----------|------------------------|
|  |                    |                                  |         |          |                        |
|  |                    |                                  |         |          |                        |
|  |                    |                                  |         |          |                        |
|  |                    |                                  |         |          |                        |
| Relevant Comments/Specific Instructions Issued |                    |                                  |         |          |                        |

# **Monitoring Business Recovery Task Progress Form**

The progress of technology and business recovery tasks must be closely monitored during this period of time. 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      | Person(s)   | Completion | n Date | Identified | Other<br>Relevant<br>Information |
|---------------------|-------------|------------|--------|------------|----------------------------------|
| (Order of Priority) | Responsible | Estimated  | Actual |            |                                  |
| 1.                  |             |            |        |            |                                  |
| 2.                  |             |            |        |            |                                  |
| 3.                  |             |            |        |            |                                  |
| 4.                  |             |            |        |            |                                  |
| 5.                  |             |            |        |            |                                  |
| 6.                  |             |            |        |            |                                  |
| 7.                  |             |            |        |            |                                  |
|                     |             |            |        |            |                                  |

#### **Preparing the Business Recovery Report Form**

On completion of business recovery activities, the business recovery team 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 business recovery team, 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 the following:

- A description of the incident
- People notified of the emergency
- Dates people were notified
- 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 critical 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. In particular, any estimate of the timing to return to normal working operations should be announced with care. It is also important that only authorized personnel deal with media gueries.

| Groups of Persons or Organizations | Persons Selected To Coordinate Communications to Affected Persons / Organizations |  |  |  |  |  |
|------------------------------------|---|--|--|--|--|--|
| Affected by<br>Disruption          | Name Position Contact Det   |  |  |  |  |  |
| 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 in order 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 in order 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:  |
| Date:  |
| (Any relevant comments by the business recovery team leader in connection with the     |
| return of this business process should be made here.)                                  |
| Total II of this business process chedia so made nore.                                 |
|  |
|  |
|  |
|  |
| I confirm that above business process is now acceptable for normal working conditions. |
|  |
| Name:  |
|  |
| Title.   |
| Title:   |
|  |
| Signature:   |
| orginatoro.  |
|  |
| Date:  |
| Dato.  |