



the dr&pw

Department:  
Roads and Public Works  
NORTHERN CAPE PROVINCE  
REPUBLIC OF SOUTH AFRICA

# **DEPARTMENTAL INFORMATION TECHNOLOGY (IT) DISASTER RECOVERY PLAN**

Version 2  
(Reviewed in March 2015)

## Table of Contents

Information Technology Statement of Intent.....	4
Policy Statement.....	4
Objectives.....	4
Key Personnel Contact Info .....	5
External Contacts .....	6
1 Plan Overview.....	7
2 Emergency Response.....	8
3 Media.....	10
4 Insurance.....	11
5 Financial and Legal Issues.....	12
6 DRP Exercising.....	12
Appendix A – Technology Disaster Recovery Plan Templates.....	13
Appendix B – Suggested Forms .....	15
Damage Assessment Form.....	16
Management of DR Activities Form.....	16
Disaster Recovery Event Recording Form .....	17
Disaster Recovery Activity Report Form.....	17
Mobilizing the Disaster Recovery Team Form.....	18
Mobilizing the Business Recovery Team Form .....	18
Monitoring Business Recovery Task Progress Form.....	19
Preparing the Business Recovery Report Form .....	19
Communications Form.....	20
Returning Recovered Business Operations to Business Unit Leadership.....	20
Business Process/Function Recovery Completion Form.....	21

## 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. This document summarizes our recommended procedures. In the event of an actual emergency situation, 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

DRPW has approved the following policy statement:

- The department 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

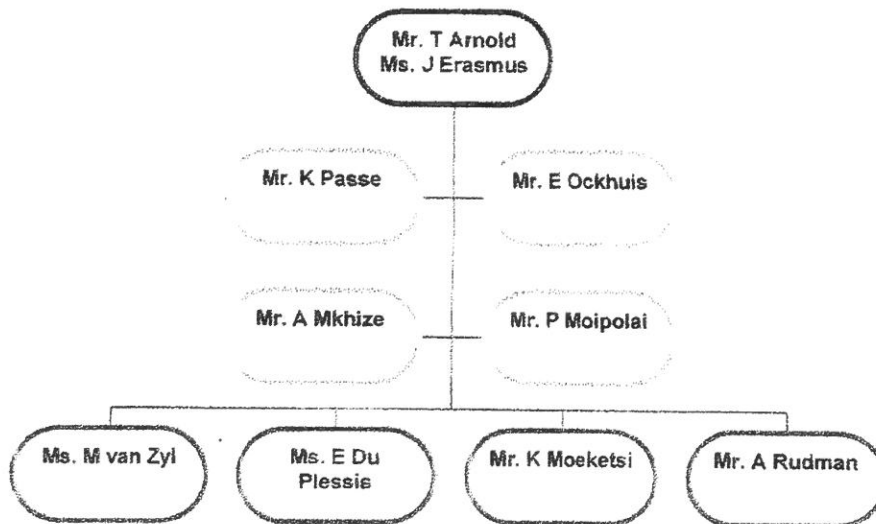
The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the department recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business 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, suppliers and others
- The main suppliers to the Department are:
  1. SITA – Provincial WAN
  2. Provincial IT – Email Servers
  3. Provincial Treasury – BAS, PERSAL, LOGIS
  4. Microzone – ProMan – Web Based Project Management Application
- IDENTIFICATION OF KEY IT BUSINESS FUNCTIONS
  5. Transversal Systems – BAS-30 users, PERSAL – 24 users, LOGIS – 15 users
  6. Departmental Internal Systems e.g. IT Service Desk, Asset register, Projects etc.
  7. Computer Hardware and User Work Related Files Backups
  8. Network equipment

### Key Personnel Contact Info

Component	Representative	System	Contact Details
IT	Mr. T Arnold	Network & Server Environment	0823489150
IT	Ms. J Erasmus	Network & Server Environment	0827428066
Chief Director	Mr. B Slings	Institutional Support	0832835573
Director	Mr. P Moipolai	Institutional Support	0718540722
CFO	Ms. F Tsimane	Finance	0784604413
Provincial IT	Mr. K Passe	Provincial Network	053 8382721
Finance	Ms. M van Zyl	PERSAL	0825636673
Finance	Ms. E Du Plessis	BAS	0842020289
Records	Ms. Z Dibeco	Registry	0765988137
Security	Mr. A Mkhize	Physical Security	0746888054
Supply Chain	Mr. K Moeketsi	LOGIS	0820507003
Supply Chain	Ms. A Swanepoel	LOGIS	0723200899
HR	Mr. A Rudman	PERSAL	0824558708
Provincial Treasury	Mr. E Ockhuis	BAS, PERSAL, LOGIS	053 8308274

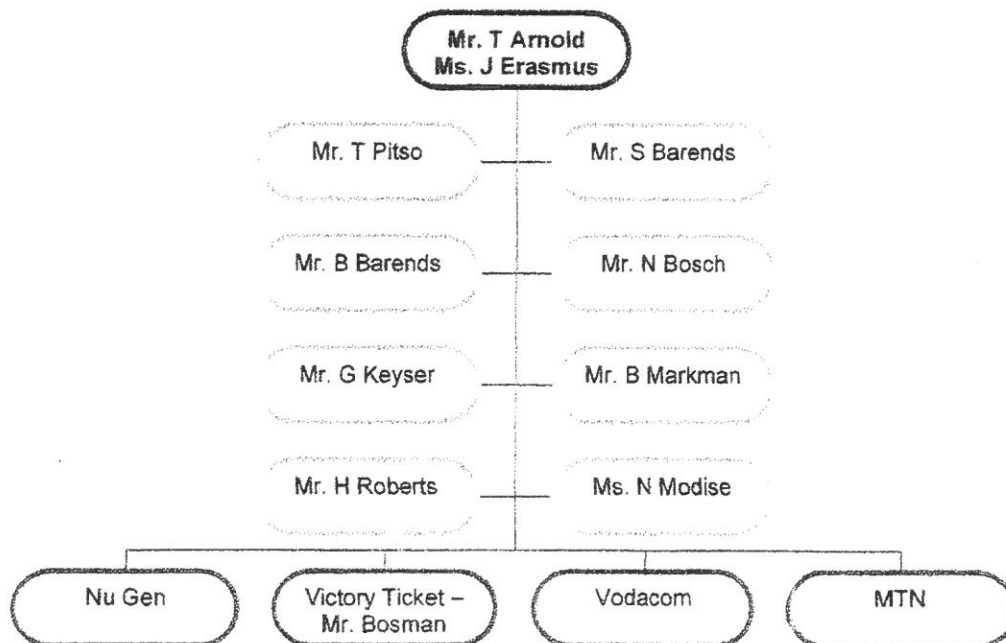
### Notification Calling Tree



### External Contacts

NAME, TITLE	CONTACT NUMBER
<b>District Managers</b>	
Francesbaard – Mr. T Pitso	0720645223
Southern Life – Mr. B Barends	0732091011
Fleet – Mr. N Bosch	0832558830
Siyanda – Mr. G Keyser	0728292098
Pixley ka Seme – Mr. B Markman	0828802364
Namakwa – Mr. H Roberts	0822255571
John Toalo Gaetsewe – Ms. N Modise	0827870912
<b>Telecom - Landline</b>	
Nu Gen	0538028900
<b>Telecom - Mobile</b>	
Vodacom	Customer Care
MTN	Customer Care
<b>Site Security</b>	
Victory Ticket – Mr. Bosman	0724606521

### External Contacts Calling Tree



[illegible]

## 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 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 Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	4	4	Not all critical equipment is located on Ground Floor, although the Main Server Room is, but has detection and raised floor.
Fire	4	4	Suppression system installed in main server room.
Act of terrorism	5		
Act of sabotage	5		
Electrical power failure	3	3	Redundant UPS array together with auto standby generator that is tested monthly.

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 DRP are:

- 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 – Parking lot of Department
- Alternate – Far end of main parking lot – Visitors Parking

#### 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 Department, 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 3 business hours;
- Restore key services within 6 business hours of the incident;
- Recover to business as usual within 8 to 24 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

- Mr. B Slingers – Chief Director
- Mr. T Arnold - IT
- Ms. C Robertson - Communications

If not available try:

- Mr. A Mkhize - Security
- Mr. B Barends

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 IT **staff** and senior representatives from the main business units. The BRT Leader will be a senior member of the



Departments management team, and will be responsible for taking overall charge of the process and ensuring that the Department 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 units. In addition, management team members will have a hard copy of the Departments disaster recovery and business continuity plans on file in their homes in the event that the head office 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 Departments 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 *emergency hotline listed in the DRPW 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 Site**

If necessary, the hot site at Roads / Southern Life / Fleet will be activated and notification will be given 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.

### **2.3.7 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

Ms. C Robertson - Communications

### 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 Departments 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 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 Department. The assessment should include:

- Loss of financial documents
- Loss of revenue / services
- Theft or Loss of equipment, documentation etc.
- Loss of cash

### 5.2 Financial Requirements

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

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for Suppliers, Salaries, Transversal Systems, etc.

### 5.3 Legal Actions

The Departments 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 Department 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.

This policy is Approved / ~~Not Approved~~  
Comments:

.....

.....

.....

.....

.....

  
HEAD OF DEPARTMENT

16/04/2015  
DATE

## **APPENDIX A – TECHNOLOGY DISASTER RECOVERY PLAN TEMPLATES**

### **Disaster Recovery Plan for DRPW – End User File System**

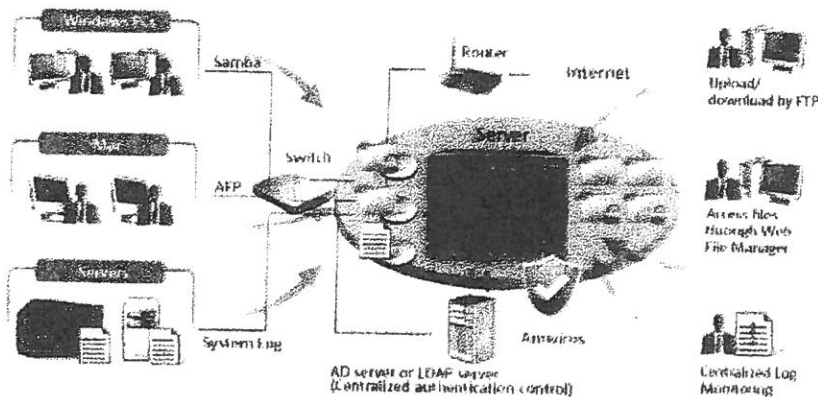
The DRPW utilizes Centralized Storage and File Sharing for the End Users and Removable drives for all Senior Managers.

#### **Cross-platform Sharing with Antivirus**

The File Servers supports SMB/CIFS, NFS, and AFP protocols for file sharing across Windows, Mac, Linux/UNIX networks. User accounts and shared folders can be created via the user-friendly web-based interface without IT expertise. The integrated antivirus solution for the File Servers ensures business continuity by offering detection against the latest viruses, malware, worms, and Trojan horses.

#### **Centralized Log Monitoring**

A central repository of log data from various network devices allows efficient management and security auditing in a businesses. The File Servers Syslog server allows the IT administrator to effectively collect and store logs of other network devices in the File Server.



#### **Senior Managers**

Senior Managers My Documents is synchronized to the Removable Drive with the proprietary software that comes with the drive.

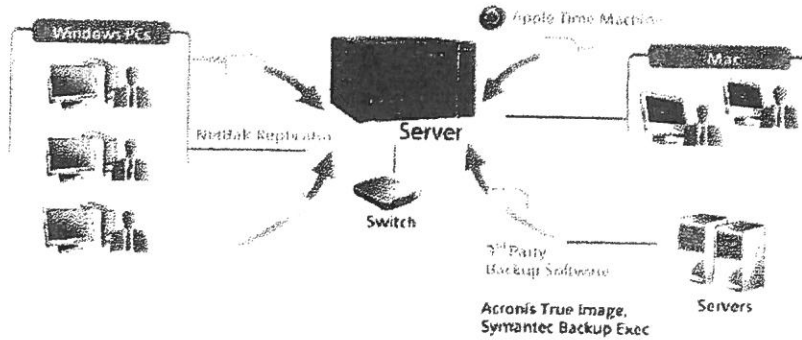


### End users File Management

The **DRPW** uses File Servers as a Backup Center for all their Business needs.

The File Servers offers a complete backup solution for businesses with NetBak Replicator which supports real-time and scheduled data backup from Windows PCs.

End users access their files by using *Drive Mapper* to connect to a shared drive on the File Server. On the File Server they will each have a personal folder and work related folders. Their personal documents are synchronized to their personal folder using NetBak Replicator.

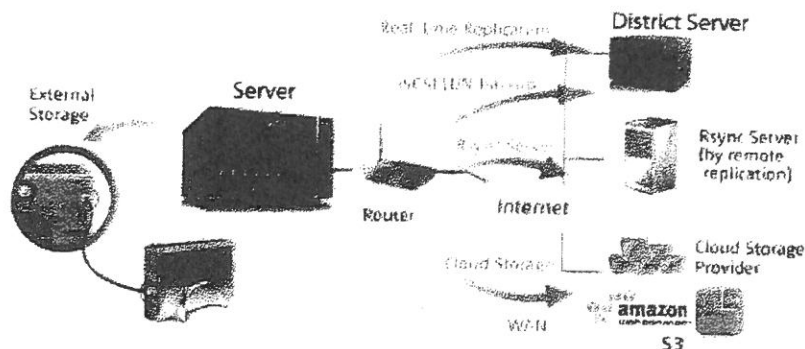


### Disaster Recovery Solution

The **DRPW** uses File Servers to offer users peace of mind, business continuity, and high availability of data by providing the ability to recover their data from disasters.

### Real-time Remote Replication

Real-time Remote Replication (RTRR) provides real-time or scheduled data replication between the Main Department Server and a remote District Server, an FTP server, or an external drive.



### **Disaster Recovery Plan for Transversal System – BAS, PERSAL & LOGIS**

Transversal Systems – Ensure minimum required access to all transversal systems. These include the availability of a remote site to access transversal systems, backup equipment to access systems and sufficient network connectivity to allow access to the transversal systems.

These systems belong to National Treasury. The possibility to loose the information is due to a disaster at any of our offices since the database is in Pretoria. We have all these transversal systems in our district offices and head office. In case of a disaster the department will still be able to process documents at one of these offices. In case that our line is down we would be able to process at provincial treasury.

It is the responsibility of the DRPW to provide laptops to the 3 directorates that will be utilized in case of a disaster.

Provincial Treasury has the responsibility to provide a Disaster Recovery Plan for the Transversal Systems of the Province.

### **Disaster Recovery Plan for Local Area Network (LAN)**

The DRPW is responsible for its own internal network.

All the Departments IT assets are captured in or by our Spiceworks IT service desk. Spiceworks also maps our complete network. All computers, printers & photocopier inventories are captured and assigned to an end user.

The IT unit also has a complete list of all BAS, PERSAL & LOGIS users. We also monitor and backup the AppWizard application that is used by Assets Management. The other software and end users that is monitored is ProMan, the project management web application and WinSMS that is used by all secretaries.

The IT unit also keeps extra network cable, switches and other network equipment for day to day use and emergencies.

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

The WAN is the responsibility of SITA ( State Information Technology Agency ). If the Transversal systems go down the IT staff will relocate specific members of the affected Transversal systems to one of the Departments functional sites, like Roads, Southern Life or Fleet. Disaster laptops will be issued and setup with our emergency network equipment. The IT staff will oversee this process.

### **Disaster Recovery Plan for Remote Connectivity**

Remote Connectivity is only allowed through SITA via any of our 3G Internet (Cell Company) providers.

### **Disaster Recovery Plan for Voice Communications**

Voice Communications is the responsibility of the Departments Communication Unit.

### **Disaster Recovery Plan for Electronic Communications**

The email system is the most vital system for all end users. This ownership of this system lies with the Provincial IT Department. If any site is down you are still able to receive your email via a 3G card using the web interface.

### Damage Assessment Form

### Management of DR Activities Form

- |                    |
|--------------------|
| Activity Name:     |
| Reference Number:  |
| Brief Description: |

[illegible]

**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.

<b>Description of Emergency:</b>					
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.

<b>Description of Emergency:</b>					
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 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 (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.
- In particular, 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 department 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 departments recovery process lead.
- It is assumed that department 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 department's 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)	
<p>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.</p> <p>Business Recovery Team Leader Name: _____</p> <p>Signature: _____</p> <p>Date: _____</p> <p>(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)</p>	
<p>I confirm that above business process is now acceptable for normal working conditions.</p> <p>Name: _____</p> <p>Title: _____</p> <p>Signature: _____</p> <p>Date: _____</p>	