Mortgageport Management Pty Ltd

IT Disaster Recovery Plan

Revision History

REVISION	DATE	NAME	DESCRIPTION
Original 1.0	22/08/2011	Annick Ah Lan	Initial IT DRP

Table of Contents

Information Technology Statement of Intent

This document delineates our policies and procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and the telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency 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

Corporate management has approved the following policy statement:

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

Objectives

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

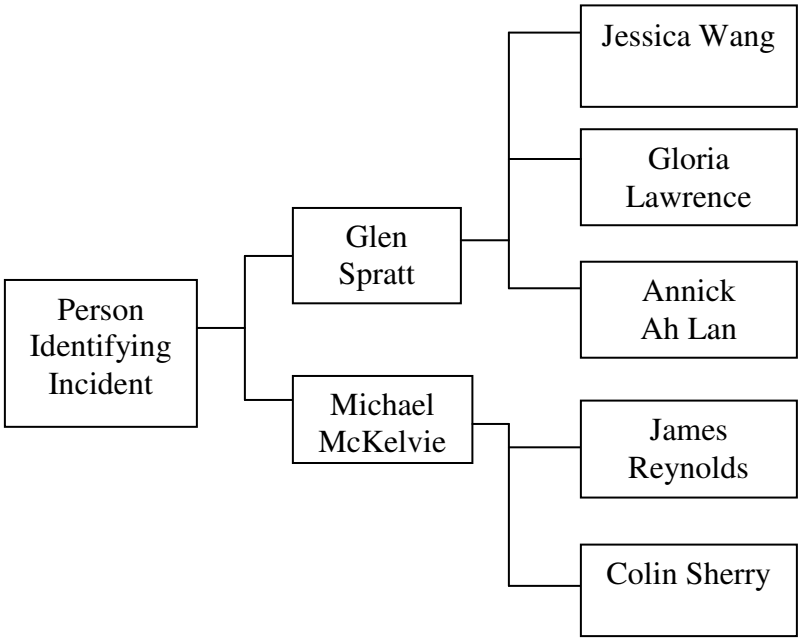
- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

Key Personnel Contact Info

Name, Title	Contact Option	Contact Number
Glen Spratt, Managing Director	Work	02 9466 8230
	Alternate	02 9466 8220
	Mobile	0411 858 886
	Home	
	Email Address	gspratt@mortgageport.com.au
	Alternate Email	
Michael McKelvie, 2IC	Work	02 9466 8213
	Alternate	02 9466 8220
	Mobile	0413 156 717
	Home	02 9386 0567
	Email Address	mmckelvie@mortgageport.com.au
	Alternate Email	
Gloria Lawrence, Client Services Manager	Work	02 9466 8217
	Alternate	02 9466 8220
	Mobile	0409 656 059
	Home	02 9712 0769
	Email Address	glawrence@mortgageport.com.au
	Alternate Email	
Jessica Wang, Financial Accountant	Work	02 9466 8221
	Alternate	02 9466 8220
	Mobile	0432 728 282
	Home	
	Email Address	jessica.wang@mortgageport.com.au
	Alternate Email	
Annick Ah Lan, Operations Manager	Work	02 9466 8228
	Alternate	02 9466 8220
	Mobile	0400 829 988
	Home	
	Email Address	aahlan@mortgageport.com.au
	Alternate Email	
James Reynolds, Sales & Marketing Manager	Work	02 9466 8206
	Alternate	02 9466 8220

Name, Title	Contact Option	Contact Number
	Mobile	0434 313 138
	Home	
	Email Address	jreynolds@mortgageport.com.au
	Alternate Email	
Colin Sherry, Portfolio Manager (Underwriting &Client Services)	Work	02 9466 8225
	Alternate	02 9466 8220
	Mobile	
	Home	
	Email Address	csherry@mortgageport.com.au
	Alternate Email	

Notification Calling Tree



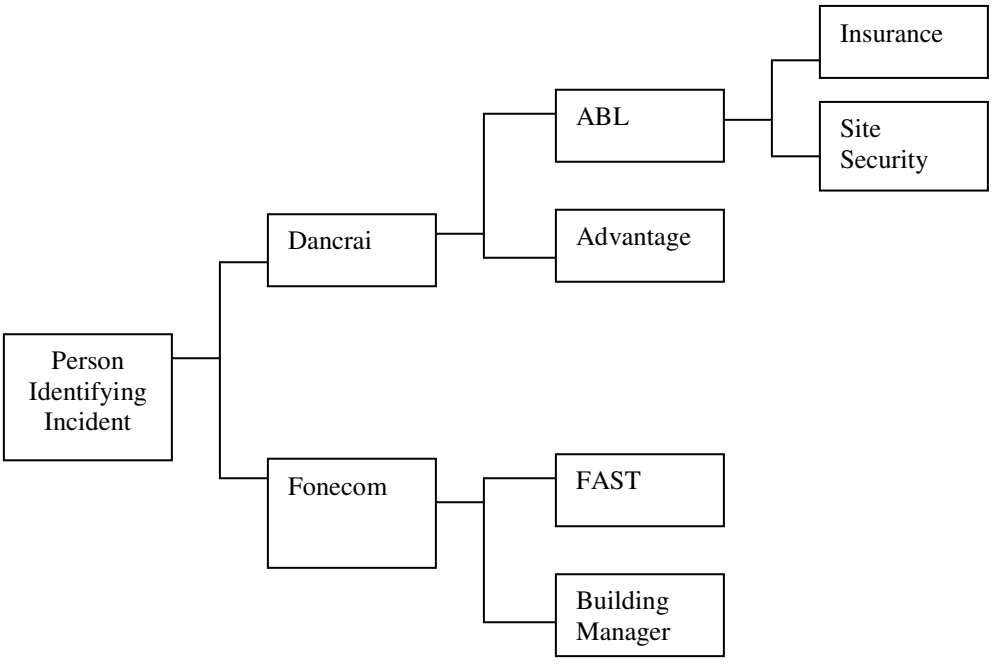
External Contacts

Name, Title	Contact Option	Contact Number
Landlord / Property Manager	Strata Choice	Derek Brien
Account Number None	Work	
	Mobile	0416 832 045
	Email Address	
Power Company	AGL	
Account Number	Work	133 835
	Mobile	
	Email Address	
Mobile Phone Carrier	Vodafone	
Account Number	Work	135888
	Mobile	
	Fax	
	Email Address	
Telephone Systems	Fonecom	Nick Criniti
Account Number	Work	02 9750 9033
	Mobile	0418 413 333
	Email Address	nick@fonecom.com.au
IT Support	Dancrai	Brad Van Der Reest
Account Number	Work	02 8905 1400
	Mobile	0409 309 9996
	Emergency Reporting	1300 30 82 30
	Email Address	bradv@dancrai.com.au
IT Equipment Supplier	Dancrai	Grant Bozier
Account Number	Work	02 8905 1400
	Mobile	
	Fax	02 8905 1401
	Email Address	grantb@dancrai.com.au
CRM/Loan Management	LoanWorks	Andrew Duerden/Iain Pallot
Account Number	Work	02 9436 1311
	Mobile	Andrew: 0403 048 757
	Mobile 2	Iain: 0450 208 428
	Email Address	andrewd@loanworks.com.au
	Email Address 2	iainp@loanworks.com.au
Office Supplies	Office Choice	
Account Number	Work	02 9906 1383

Name, Title	Contact Option	Contact Number
	UserID	esalway@mortgageport.com.au
	Password	MOR007
	Email Address	sales@capital-office.com.au
Insurance – Professional Indemnity	Nova Underwriting Pty Ltd (InterRISK Australia)	Alan Lyne
Policy No: 190527	Work	02 9949 2744
	Email Address	
Insurance – Worker's Compensation	Employers Mutual NSW Limited	
Policy No: 20WOR0109897122	Work	02 8251 9000
	Email Address	
Insurance – Building and Contents	CGU Insurance Limited (Brookvale Insurance Brokers Pty Ltd)	
Policy No: 15T0858292	Work	02 9934 9700
	Mobile	
	Email Address	insurance@bib.com.au
Insurance – Broker	InterRISK Austarlia	Mark Winwood
	Work	02 9346 8086
	Mobile	
	Email Address	mark.winwood@interrisk.com.au
Site Security –	Kings Security	Sally Liljeqvist
Account Number	Work	02 9310 1888
	Mobile	
	Email Address	managed.services@kingssecurity.com.au
Off-Site Storage	Access Records	
Account Number 70058	Work	02 9666 7744
	Fax	02 9666 7944
	Email Address	
Telecom Supplier	Primus Telecom	
Account Number	Work	1300 85 66 88
	Mobile	
	Email Address	

Name, Title	Contact Option	Contact Number
Aggregator	FAST	James Ashdown
Account Number	Work	02 9233 8222
	Mobile	0437 399 096
	Email Address	james.ashdown@fastgroup.com.au
Lender 1	Adelaide Bank	Fons Caminiti
Account Number	Work	08 8220 7409
	Mobile	
	Email Address	fcaminiti@adelaidebank.com.au
Lender 2	Advantedge	Peter Colnan
Account Number	Work	02 9560 2794
	Mobile	0422 391 230
	Email Address	peter.colnan@advantedge.com.au
Banking	ANZ	Athena Eliopoulos
	Work	02 9329 7200
	Mobile	
	Email Address	

External Contacts Calling Tree



1 Plan Overview

1.1 Plan Updating

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

1.2 Plan Documentation Storage

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

1.3 Backup Strategy

Key IT business processes and the agreed backup strategy for each are listed below. The main strategy chosen is for a backup tape to be made at the end of each working day. This tape is then taken off-site at a pre-determined location at least 5 kilometres away from the office premises and brought back the next morning. The daily tapes are rotated on a per-weekly basis for four consecutive weeks. This strategy entails the maintenance of backup tapes which will enable a full disk recovery from the previous day's daily activities or from any specific date for up to 4 weeks from the date of incidence. Backup logs are kept and reviewed on a regular basis. All backup failures and restorations from a backup are noted in the log. This may help identify and prevent future backup problems. The majority of our IT operations are also outsourced to 3rd party suppliers which means that either the data is stored off-site or we would mirror the supplier's IT disaster recovery plan in the event of an incident.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Backup from tape, outsourced services to 3rd party
Tech Support - Hardware	Outsourced services to 3rd party
Tech Support - Software	Outsourced services to 3rd party
Facilities Management	Backup from tape
Email	Backup from tape, outsourced services to 3rd party
Purchasing	Outsourced services to 3rd party
Disaster Recovery	Outsourced services to 3rd party
Finance	Backup from tape
Contracts Admin	Backup from tape
Warehouse & Inventory	Off-site storage facility
Product Sales	Outsourced services to 3rd party
Human Resources	Backup from tape
Web Site	Off-site 3rd party server facility

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 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.

1.4.1 External Risks

External risks are those that cannot be associated with a failure within the company. They are very significant in that they are not directly under the control of Mortgageport. External risks can be split into four subcategories:

- Natural: These disasters are on top of the list. Typically they will damage a large geographical area. To mitigate the risk of disruption of business IT operations, our recovery solution involves continuation of business as usual activities from the home environment. Nowadays most of the meteorological threats can be forecasted, hence the chances to mitigate the effects of some natural disasters are considerable.
- Human Caused: These disasters include acts of terrorism, sabotage, virus attacks, operation mistakes, crimes, etc. These can be caused by both internal and external persons.
- Civil: These risks typically are related to the location of the business facilities. Typical civil risks include labour disputes ending in strikes, communal riots, local political instability, etc. These again may be internal to the company or external.
- Supplier: These risks are tied to the capacity of suppliers to maintain their level of services in a disaster. We will maintain a backup supplier pool in case of emergency.

1.4.2 Facility Risks

Facility risks are risks that affect only local facilities. While evaluating these risks, we will consider the following utilities and commodities:

- Electricity
- Telephones
- Water
- Climate control
- Fire
- Structural
- Physical security

1.4.3 Data Systems Risks

Data systems risks are those related to the use of shared infrastructure, such as networks, file servers and software applications that could impact multiple departments. Data system risks can be evaluated with the following subcategories:

- Data communication network
- Telecommunication systems and network
- Shared servers
- Virus
- Data backup/storage systems
- Software applications and bugs

Potential disasters have been assessed as follows for the items that deserve the most attention from the above:

Potential Disaster	Probability Rating	Impact Rating	Restoration Time	Brief Description Of Potential Consequences & Remedial Actions
External Risks				
Flood	1	4	5	No access to office premises, work from home
Fire	2	4	5	Fire and smoke detectors on all floors throughout the building and the office, evacuation of premises and eventual restoration of business as usual activities depending on extent of damage. Otherwise work from home.
Act of terrorism	1	3	4	Immediate notification of emergency services and depending on the nature of the act of terrorism and extent of damage – re-establishment of essential services, restoration of business as usual activities and full cooperation with relevant authorities and government.
Act of sabotage	1	3	4	Appropriate screening process in place for all employees including background checks and references. Doors are locked with a unique passcode at all times during business hours. Alarm system monitored by 3rd party after-hours. Depending on nature of failure and extent of damage – eventual restoration of business as usual activities within allowable timeframe.
Facility Risks				
Electrical power	2	2	2	UPS that is tested weekly &

failure				remotely monitored 24/7. Depending on extent of failure, eventual restoration of business as usual activities, otherwise work from home.
Loss of voice communications network services	2	2	2	Provider monitors voice communications systems remotely. Carrier provider to reset and divert all calls to either call centre or mobiles. All employees are required to have mobile phones to be contactable at all times.
Loss of communications network services	3	2	2	One SHDSL server connection. Depending on extent of failure, eventual restoration of business as usual activities within allowable timeframe.
Data Systems Risks				
Virus	2	2	1	24/7 Anti-virus monitoring as well as spam filtering and firewall in place. Depending on extent of virus attack, virus to be isolated and all other workstations and data systems scanned for potential threats and quarantined for elimination of virus.

Probability: 1=Very Low, 5=Very High
Impact: 1=Minor Annoyance, 5=Total Destruction
Restoration: 1=minor restoration, 5 = major restoration

2 Emergency Response

2.1 Alert, escalation and plan invocation

2.1.1 Plan Triggering Events

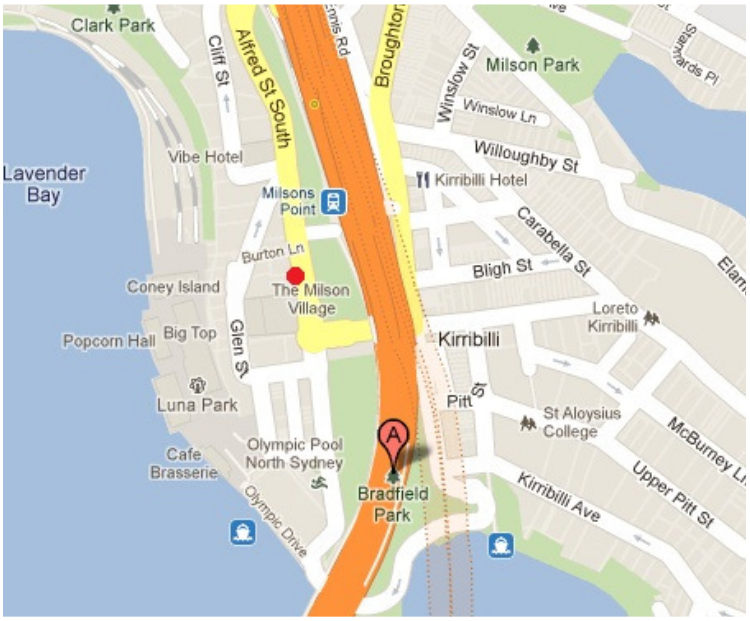
Key trigger issues at office premises that would lead to activation of the DRP are:

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

2.1.2 Assembly Points

Where the premises need to be evacuated, the DRP invocation plan identifies one primary evacuation assembly point:

- Primary – Bradfield Park



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. Responsibilities of the ERT are to:

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

2.2 Disaster Recovery Team

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

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

2.3 Emergency Alert, Escalation and DRP Activation

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

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

2.3.1 Emergency Alert

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

Emergency Response Team

- Glen Spratt
- Michael McKelvie
- Annick Ah Lan
- James Reynolds

If not available try:

- Gloria Lawrence
- Jessica Wang
- Colin Sherry

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

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

2.3.2 DR Procedures for Management

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

2.3.3 Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list are advised to call the staff member's emergency contact to relay information on the disaster.

2.3.4 Backup Staff

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

2.3.5 Updates

For the latest information on the disaster and the organization's response, staff members can call their reporting line manager for information on the nature of the disaster, assembly sites, and updates on work resumption.

2.3.7 Work Continuation

If necessary, employees will work from home and continue business as usual until the office premises is re-established. Our daily business processes are conducted via web-based applications which all employees can access by using their secure usernames and passwords. All employees are required in their contracts to have access to the Internet via a home computer or laptop.

2.3.8 Personnel and Family Notification

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

3 Media

3.1 Media Contact

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

3.2 Media Strategies

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

3.3 Media Team

- James Reynolds
- Glen Spratt
- Michael McKelvie

3.4 Rules for Dealing with Media

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

4 Insurance

As part of the company's disaster recovery and business continuity strategies a number of insurance policies have been put in place. These include workers compensation, professional indemnity, contents insurance and business interruption.

If insurance-related assistance is required following an emergency out of normal business hours, please contact: Mark Winwood on 02 9346 8086.

Policy Name	Coverage Type	Coverage Period	Amount Of Coverage	Person Responsible For Coverage	Next Renewal Date
Business Package	Fire & Perils Business Interruption Liability	1 year	$400,000 $500,000 $20,000,000	Brookvale Insurance Brokers	30/09/2011
Professional Indemnity	Professional Indemnity Insurance	1 year	$2,000,000	InterRISK	16/10/2011
Workers Compensation Insurance	Workers Compensation	1 year	Open	EmployersMutual	9/10/2011

5 Financial and Legal Issues

5.1 Financial Assessment

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

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

5.2 Financial Requirements

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

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

5.3 Legal Actions

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

6 DRP Exercising

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

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

Appendix A – Disaster Checklist

Disaster action checklist

1. Plan Initiation
    a. Notify senior management
    b. Contact and set up disaster recovery team
    c. Determine degree of disaster
    d. Implement proper application recovery plan dependent on extent of disaster
    e. Monitor progress
    f. Contact all necessary personnel--both user and data processing and establish schedules
    g. Contact vendors--both hardware and software
    h. Notify users of the disruption of service
2. Follow-Up Checklist
    a. List teams and tasks of each
    b. Obtain emergency cash ,if necessary
    c. List all personnel and their telephone numbers
    d. Establish user participation plan
    e. Set up the delivery and the receipt of mail
    f. Rent or purchase equipment, as needed
    g. Determine applications to be run and in what sequence
    h. Identify number of workstations needed
    i. Check out any off-line equipment needs for each application
    j. Check on forms needed for each application
    k. Set up primary vendors for assistance with problems incurred during emergency
    l. Check for additional magnetic tapes, if required
    m. Take copies of system and operational documentation and procedural manuals
    n. Ensure that all personnel involved know their tasks
    o. Notify insurance companies

Appendix B – Disaster Recovery for Major Systems

Disaster Recovery Plan for System One

SYSTEM	**mpm-sbs.mortgageport.loc**

OVERVIEW	Physical system for SBS 2008 – FSMO, Exchange 2007, Backup, File, DNS, DHCP
PRODUCTION SERVER	Location: Communications Room Server Model: Dell PowerEdge R710 Operating System: Windows SBS 2008 CPUs: Intel (R) Quad Core E5530 Xeon(R) CPU, 2.40 GHz, 8M Cache Memory: 12GB Memory (3x4GB) 133Mhz Dual Ranked RDIMMs Total Disk: 2 x 146 (15k SAS); 4 x 450 (15k) SAS Service Tag: 2z9p62s System Serial #: 6486171652 Gateway: 10.1.1.254 IP Address: 10.1.1.5 Other: DRAC 10.1.1.6 Purchase Date: 13/09/2010 Warranty Date: 13/09/2013 Warranty Type: 4HR (24x7), 4 hours response on-site 24x7

KEY CONTACTS	
Hardware Vendor	Dancrai
System Owners	Dancrai
Database Owner	Dancrai
Application Owners	Dancrai
Software Vendors	Dancrai
Offsite Storage	Becky Wang

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	Tape backup to be taken away from the office premises by designated person
Monthly	Tape backup to be taken away from the office premises by designated person
Quarterly	Tape backup to be taken away from the office premises by designated person

SYSTEM ONE DISASTER RECOVERY PROCEDURE	
<u>Scenario 1</u> Total Loss of Data	Restore data from previous working day from the backup tape
<u>Scenario 2</u> Total Loss of HW	Contact IT supplier to order new server, estimated delivery time is 1 week. Partially restore mission-critical data from previous working day from the backup tape to mpm-svr2 in the interim.

File Systems 17/08/2011

File System as of 17/08/2011	File system	1K-blocks	Used	Avail	%used	Mounted on	Summary(total\available)
	C	140526588	90468356	50058232	64%	/FIXED/C	134.16gb\47.75gb
	D	2100388	14216	2086172	0%	/FIXED/D	2.03gb\1.10gb
	F	1316877308	560544888	756332420	42%	/FIXED/F	1.23tb\721.30gb
Other critical files to modify	none						
Necessary directories to create	Shared paths or directories						
Critical files to restore	MYOB						
Secondary files to restore	C Drive						
Other files to restore	D Drive & F Drive						

Disaster Recovery Plan for System Two

SYSTEM	**mpm-svr2.mortgageport.loc**

OVERVIEW	Physical system for SQL (ARM server)
PRODUCTION SERVER	Location: Communications Room Server Model: IBM X Series 346 (MT-M8840-DIM) Operating System: Windows 2003 SP1 CPUs: Xeon @ 2.8Ghz Memory: 3.25 GB Total Disk: 6 x 146GB SCSI System Serial #: 99BBEXK IP Address: 10.1.1.4 Subnet: 255.0.0.0 Gateway: 10.1.1.254 HDD Configuration: c: 48.8GB 26 free; d: 88GB 76 free; e: 410 GB 86 free Purchase date: 31/07/2006 Warranty date: 31/07/2009

KEY CONTACTS	
Hardware Vendor	Dancrai
System Owners	Mortgageport
Database Owner	ARM
Application Owners	Dancrai
Software Vendors	Microsoft, ARM
Offsite Storage	Becky Wang

BACKUP STRATEGY for SYSTEM TWO	
Daily	Tape backup to be taken away from the office premises by designated person, backup is formed from mpm-sbs server
Monthly	Tape backup to be taken away from the office premises by designated person, backup is formed from mpm-sbs server
Quarterly	Tape backup to be taken away from the office premises by designated person, backup is formed from mpm-sbs server

SYSTEM TWO DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	Restore data from previous working day from the backup tape, backup is formed from mpm-sbs server.
Scenario 2 Total Loss of HW	Contact IT supplier to order new server, estimated delivery time is 1 week. Restore data from previous working day from the backup tape to mpm-sbm in the interim.

File Systems 17/08/2011

File System as of 17/08/2011	File system	1K-blocks	Used	Avail	%used	Mounted on	Summary(Total\Available)
	C	51202031	26196223	25005808	51%	/FIXED/C	48.84gb\23.86gb
	D	92170236	12279352	79890884	13%	/FIXED/D	87.92gb\76.19gb
	E	430118892	349243576	80875316	81%	/FIXED/E	410.19gb\77.13gb
Other critical files to modify	none						
Necessary directories to create	Shared paths or directories						
Critical files to restore	C Drive						
Secondary files to restore	D Drive						
Other files to restore	E Drive						

Disaster Recovery Plan for Desktop Environment

SYSTEM	Other

OVERVIEW	19 Staff including 6 laptop/mobile users
APPLICATIONS IN USE	• MS Office, Excel, Word, Outlook • RFS – Online Banking – Adelaide Bank (private WAN linked to Adelaide Bank – requires that VPN to be established with their hardware) • ARM – CRM AXCMAN installed locally SQL DB server (to be phased out over the next 3 months) • Utilise the O drive for company files • Avaya phone manager – used by Client services/receptionist to manage internal phone extensions • LoanWorks - CRM IPhones in use with Active Sync for email Desktop Anti-Virus is ESET NOD32 MYOB19, 3 users, data files on server ANZ Online – 1 user, internet banking Interspire – Mailouts There is only Ad-Hoc support for ARM with Access in Melbourne
AD Domain	mortgageport.loc
DHCP Settings	GW 10.1.1.254 DNS 10.1.1.1, 10.1.1.4

BACKUP STRATEGY	
Anytime	Spare desktop for immediate use if one desktop fails, otherwise we will need to contact IT provider to order several new desktops

DISASTER RECOVERY PROCEDURE	
<u>Scenario 1</u> Total Loss of Data	Any business data is saved on O drive, no business information is stored on hardware so no recovery option needed.
<u>Scenario 2</u> Total Loss of HW	Use spare workstation but if not available order new workstation and rebuild.

Disaster Recovery Plan for Firewall

SYSTEM	Cyberoam CR25ia

OVERVIEW	
EQUIPMENT	Location: Communications Room Model No.: CR25ia System Serial #: C047500604-8JJOF3 IP Address (internal): 10.1.1.254/24 IP Address (external): 211.26.160.155/29 Gateway: 211.26.160.153 Purchase date: 18/11/2010 Warranty date: 18/11/2013 Web Management (internal): http://10.1.1.254:8080 (HTTP) https://10.1.1.254:10443 (HTTPS) Web Management (external): https://211.26.160.155:10443

KEY CONTACTS	
Hardware Vendor	Dancrai
System Owners	Dancrai
Database Owner	Dancrai
Application Owners	Dancrai
Software Vendors	Dancrai
Offsite Storage	Dancrai
Network Services	Dancrai

BACKUP STRATEGY	
Daily	When a change is implemented, the new configuration is backed up
Monthly	When a change is implemented, the new configuration is backed up
Quarterly	When a change is implemented, the new configuration is backed up

DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Network	n/a
Scenario 2 Total Loss of HW	In case of hardware failure, another device could be ordered with the same configuration and loaded with the backed up configuration of the failed firewall.

Disaster Recovery Plan for Voice Communications

SYSTEM	**Avaya IP Office**

OVERVIEW	
EQUIPMENT	Location: Communications Room Device Type: PABX Model No.: IPO 500 Network Interfaces: ISDN IP Address: 10.1.1.11

KEY CONTACTS	
Hardware Vendor	AVAYA
System Owners	Mortgageport
Database Owner	Mortgageport
Application Owners	Mortgageport
Software Vendors	Avaya
Offsite Storage	Fonecom
Network Services	Primus

BACKUP STRATEGY	
Daily	Database on mpm-svr2
Monthly	Database on mpm-svr2
Quarterly	Database on mpm-svr2

DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Switch	Carrier Provider to divert all calls to either Call Centre or Mobiles
Scenario 2 Total Loss of Network	n/a

Appendix C – Suggested Forms

Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

_____

Management of DR Activities Form

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

Activity Name:
Reference Number:
Brief Description:

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

_____

Disaster Recovery Event Recording Form

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

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

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

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

_____

Disaster Recovery Activity Report Form

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

The report will include:

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

_____

Mobilizing the Disaster Recovery Team Form

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

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

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

_____

Mobilizing the Business Recovery Team Form

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

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

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required

Relevant Comments (e.g., Specific Instructions Issued)					

_____

Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period 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	Gloria Lawrence	Client Services Manager	0409 656 059
Management & Staff	Michael McKelvie	2IC	0413 156 717
Suppliers	Gloria Lawrence	Client Services Manager	0409 656 059
Media	James Reynolds	Sales & Marketing Manager	0434 313 138
Stakeholders	Glen Spratt	Managing Director	0411 858 886
Others	Annick Ah Lan	Operations Manager	0400 829 988

_____

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: _____

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

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

Name:
_____

Title:
_____

Signature:
_____

Date: _____