Appendix A: BIA Form

Business Impact Analysis Form

Date: _____ **Department:** _____

Business Unit: _____ **Business Function:** _____

List the most critical resources that you need in order to sustain your mission for the first week.

a. Work area space: _____

b. Workstation / P.C. / Printer: _____

c. Telephone / Network: _____

d. Other: _____

List of applications that support this business function that will require recovery in the event of a disaster.

1. _____
2. _____
3. _____
4. _____

A. FINANCIAL IMPACT

What would the total cumulative dollar loss be for each time element; include estimated overtime, fines, etc. (Do not include income which was delayed, but not lost.) Please note the rationale in comments area.

1.	RM0	-	RM50k	4.	RM500k	-	RM1000k
2.	RM50k	-	RM200k	5.	RM1000k	-	RM5000k
3.	RM200k	-	RM500K	6.	RM5000k	-	Above

1 Hr	12 Hrs	24 Hrs	72 Hrs	1 week	1 month
_____	_____	_____	_____	_____	_____

Comments:

_____

_____

B. CUSTOMER IMPACT/VISIBILITY

How would the loss of this application appear from the external or internal customer's point of view?

1. Not Visible
2. Slight Impact
3. Moderate Impact
4. Extreme Impact
5. Critical Impact
6. Catastrophic

1 Hr	12 Hrs	24 Hrs	72 Hrs	1 week	1 month

Comments:

C. LEGAL IMPACT

What would the legal impact be of this outage, i.e. broken customer or other legal contracts, government commitments, etc?

1. Not Visible
2. Slight Impact
3. Moderate Impact
4. Extreme Impact
5. Critical Impact
6. Catastrophic

1 Hr	12 Hrs	24 Hrs	72 Hrs	1 week	1 month

Comments:

D. CORPORATE IMPACT OF OUTAGE

What would be the overall impact to company corporate image, reputation and share holder confidence caused by the loss of this data to the business function?

1. Not Visible
2. Slight Impact
3. Moderate Impact
4. Extreme Impact
5. Critical Impact
6. Catastrophic

1 Hr	12 Hrs	24 Hrs	72 Hrs	1 week	1 month
____	____	____	____	____	____

Comments:

D. OTHERS

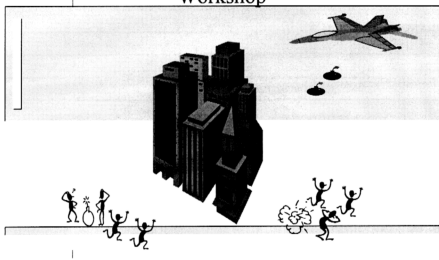
What other areas of business would be impacted by this data / application inability to process for a 24 hour period or more?

Comments:

Appendix B: Disaster Recovery Checklist

I. Business Recovery Priority	Check Off
1. Was a Business Impact Assessment done?	Y / N
2. Have a business-driven application, data recovery sequence and time frame been developed, documented and reviewed with the affected business?	Y / N
3. Has the management of the supported business area reviewed the planned recovery process and time frame and have they agreed to the plan?	Y / N
II. Information Backup	
1. Is all BUSINESS CRITICAL (or even better, ALL) data backed up and stored off-site?	Y / N
2. Based on how often the data is backed up and transported off-site, is the potential worst case risk of data loss acceptable to the supported business and agreed upon by management?	Y / N
3. Is the backup documentation stored off-site with the data?	Y / N
4. Is the off-site storage location sufficiently distant from the primary site to be considered "safe"?	Y / N
III. Disaster Recovery Plan	
1. Is the plan totally self-sufficient and able to stand alone? (Does it contain ALL of the information and documentation necessary to facilitate and manage the recovery?)	Y / N
2. Is the recovery plan written so that unfamiliar technical staff can understand and execute it?	Y / N
3. Is the plan classified as "Confidential Proprietary"?	Y / N
IV. Testing The Plan	
1. Has the plan been tested?	Y / N
2. Were the system, network and critical applications recovered within the agreed upon parameters (e.g. time frame)?	Y / N
3. Was the completeness of the recovery verified by the business or applications support areas?	Y / N
4. Did all materials for the test (i.e. backed up data, documentation and recovery procedures) come from off-site locations?	Y / N
5. Was a detailed test log kept which listed the problems that were encountered and ideas for improvement?	Y / N
6. Was the test done using staff who were unfamiliar with this site and their systems and applications?	Y / N
7. Were the results of the tests and the planned corrective actions documented and presented to the business area management?	Y / N

Welcome to the Disaster Recovery Workshop



Objective of DR Planning

To ensure that the continuity of MCSB's business operations in the event of unanticipated computer processing disruptions such as operational failures or site disasters that destroy or prevent access to the computer equipment, data and software

Please comment on any other areas of concern which should be considered when assessing a major network outage.

Comments:

Summary of the processes involved

- Establish criticality of each application and system to the business
- Plan and implement data backup and recovery based on criticality
- Store data,documentation of data and recovery plan off-site
- Test the plan confirming recovery within business-driven time frame

Review,test and update plan annually

Who performs the DR Planning

- Systems owners and users
- Equipment and network custodians

Your Role / Duties

- Follow direction and priorities set by management
- Responsible for the development,implementation, monitoring,maintenance and testing of the DR Plan

Who will work with you

- Disaster Recovery Co-ordination Team
- Management
- Department/Operations which owns application, device,system or information
- Department/Operations that would be impacted by the loss of the application, device,system or information

Select Recovery Options and Strategies

- Identify recovery method
- Determine recovery location and facility
- Identify hardware,software and network requirements
- Examples of strategies include :
  - *the possibility of using other systems in the network
  - *purchase/rent new equipment's
  - *rent space
  - *identify alternative site for possible transfer of operations
  - *agreements with other departments / organizations

Basis for recovery process

- How fast the application need to be recovered
- How much data can business afford to lose
- Difficulty of replacing or recreating data
- Frequency of changes to the data - daily,weekly,monthly,quarterly
- Consideration on cost of recovery strategy

Important !!!

Ensure that the review strategy, cost, it's pros and cons are documented and approved by the management

Establish Back-up and Records Retention Plan

The requirements are :

- Do full backup weekly
- Do incremental backups daily or more as required by business
- Keep backup information and documentation physically separate from system
- Select and off-site location which in not subject to similar risks
- Keep copies of backups near the site storage

Develop a Disaster Recovery Plan

What are the information needed in a Disaster Recovery Plan ????

Components of a DR Plan

- Recovery Staff / Teams
- Incident Notification Process
- Recovery Facilities
- Recovery Plan
- Backup/Restore Procedures
- Special Forms and Supplies Lists
- Vendors/ Suppliers Lists
- Inventory and Required Information
- Master Phone Lists

Identify Recovery Staff and Teams

Would consist of :

- Systems administrators
- Technicians
- Engineers
- Departmental Managers
- Operational Managers

Recovery Facilities

This section documents the locations, phone numbers, hardware, software and activation procedures of a prearranged recovery location. The criteria for selecting a location is based on the criticality of the business supported and this in turns determines the speed of recovery expected

Identify Recovery Staff and Teams

Would consist of :

- Systems administrators
- Technicians
- Engineers
- Departmental Managers
- Operational Managers

Recovery Facilities

This section documents the locations, phone numbers, hardware, software and activation procedures of a prearranged recovery location. The criteria for selecting a location is based on the criticality of the business supported and this in turns determines the speed of recovery expected

Disaster Recovery Plans

This section would document all of the step by step action points and procedures that would need to be performed at the recovery site in order to restore the computer system concerned.This includes full hardware, software, operating system,cabling and network requirements.The detailed steps used to recover the system and application as well as operating procedures and documentation are also contained in this section.Also included in this section is the priority lists on the crucial applications to be developed first and the users that are provided with access first depending on their criticality

Backup and Restore Procedures

This section documents the daily, weekly and monthly backup schedule procedures. It also contains the procedures on how to restore the backed up data as well as how to recall the off-site tapes.

Special Forms and Supplies Lists

This lists contained in this section will be used to gather any special forms, manuals and supplies that are kept at off-site locations for the transport to the recovery site

Vendor Lists

This section lists all vendors i.e., hardware,software,network,support services ,etc. which might need to be contacted in the event of a disaster.Document full corporate names, addresses, day and night phone and FAX numbers.Also list names and phone numbers of sales support and services staff.

Inventory and Required Information

This section contains miscellaneous documentation such as hardware,software and network configurations, an inventory of equipment's and applications, warrantee information, etc.A Disaster Recovery Manual Update procedures which includes a list of who has each Disaster Recovery Manual for control and update purposes and a contents/check-off list of what is stored off site and would have to be relocated in the event of a disaster. A current list of changes made to the system could be very helpful during the recovery process

Master Phone Lists

This section lists the business, home and pager numbers of all personnel who might need to be contacted in the event of a disaster .List police and fire departments, hospitals, airlines,hotels, etc. Also included are the phone numbers for phones and FAX equipment located at the recovery site or alternate operation facilities.

Features of a Disaster Recovery Plan

- Simple to understand
- Procedures organized sequentially throughout recovery process
- Can be easily maintained and modified
- Contains all information necessary to ensure successful recovery

Appendix D: Standard Operation Procedure

A. Information backup and recovery standards

Purpose

To state the MCSB Information Backup/Recovery standards for the protection of computer based information. MCSB's essential business functions are highly dependent on our computerised systems. The backup and safe storage of information is fundamental to the reliability and recoverability of each system and its supported businesses. In the event of information corruption or loss, disk hardware failure or site disaster, the backup information is often **only link to recovery**.

Responsibilities

The custodians of the computer applications, equipment and facilities in co-ordination with the application system owners." Custodians are identified as the ones who are "responsible for the operation and maintenance of the data processing equipment." Systems owners are identified as the "user or group of users with the primary responsibility for updating the application files."

These Information Backup/Recovery standards define requirements which must assist in providing for a timely recovery of MCSB's critical business activities when an outage or a disaster occurs. Information Backup and Recovery Standards, includes the following subsections:

A.1 Identifying Critical Information
A.2 Backup Requirements for Critical Business Applications
A.3 Backup Requirements for Non-Critical Business Applications
A.4 Backup Procedures
A.5 Off-Site Storage

A.1 Identifying Critical Information

The degree and scope of data recovery and backup planning is totally driven by the potential company and business impact that would result from the loss of a particular application, data, system, and/or network. An application's business criticality is based on several evaluation areas.

Customer visibility measures the impact that the loss of the application would have from the perspective of MCSB customers (e.g. loss of customer or employee good will).

Financial impact evaluates the application's business importance in terms of how its loss would effect revenue or our inability to meet financial obligations.

The legal impact rates the application's business importance in terms of legal, contractual, governmental, or regulatory requirements.

The impact to the corporate image that would result from the loss of an application and/or its data is also evaluated. Such a loss could seriously erode our corporate reputation and shareholder confidence. A major loss could cause an inability to function as a company.

The methodology used to determine the criticality of business applications, data, systems, and/or networks is the Business Impact Assessment (BIA) process. The BIA process is the most important step in both backup strategies and disaster recovery planning. In this phase, a business assessment is performed on all applications and data running on the system or network being analysed. The result of this assessment determines the criticality of the application and data to the business and to MCSB as a whole. The criticality dictates how quickly the application, data, systems and/or networks need to be recovered. This speed of recovery is then used to help design the proper recovery strategy. The BIA

process also identifies how current the recovered information will need to be in order to return the business to an operational status.

It is through this process that the business recovery requirements are defined. These requirements then provide the design objectives for the Information Backup Plan, recovery plan, as well as the recovery time frame by which the effectiveness of the disaster recovery process will be measured.

The MCSB requirements for information backup has been divided into the following two recovery groups based on business defined application criticality. Critical Business Applications, data, systems, and/or networks are those assets where the owner has determined is essential in order for the company to meet its customer and/or business commitments. Non-critical Business Application, data, systems, and/or networks are those assets where the owner has determined has a lesser business impact and can tolerate greater loss of data or longer recovery time in the event of a disaster.

A.2 Backup Requirements for Critical Business Applications

Because of the need for rapid recovery, often with little or no loss of data (as defined by the Business Impact Assessment process), the backup methodology, frequency and off-site storage process used for essential business applications may vary widely. Daily or more frequent backups, electronic vaulting, remote file mirroring, and standby processing must all be considered based on business need.

A Business Impact Assessment (BIA) must be performed for each business application, system, and/or network in order to establish the true level of information criticality. The criticality classification and the backup process must be reviewed/updated by the application owner and equipment custodians:

When the application changes,
When significant changes in exposure occur,
Minimum annually

The level of information criticality must be reviewed, documented and agreed upon by the affected application owners and equipment custodians. An Information Backup Plan must be developed to fully support the operating systems, software applications and data to the agreed upon level of criticality.

An Information Backup Plan must contain the name of the system and or data, frequency and type of backup, offsite vaulting cycle and any trade off rational used in developing the backup plan.

The Backup Plan must insure that in the event of a disaster, the backup information, which is stored off-site, is complete and sufficiently current so that the amount of data loss is acceptable to business management.

Based on the Backup Plan, information must be backed up on a scheduled basis and must, along with its documentation, be taken off-site frequently enough to insure that in the event of a disaster, the recovered data is current enough to support the business.

A.3 Backup Requirements for Non-Critical Business Applications

Non-critical business applications and data must be fully backed up weekly. Incremental or differential backups must be done as required by the business. Backup information must be kept physically separated from their systems, with at least one full set of backups, and associated documentation stored off site for disaster recovery purposes. System, file server software, application programs and data must have full backups taken weekly.

The backups must be kept in an area physically separate from the systems/server(s).

All backup information must be stored with its documentation in a secure location.

Incremental or differential backups must be done based on business need.

A backup copy of the system, file server software, application programs, data, documentation, and other Disaster Recovery records must be kept in an off-site location.

Users of portable and/or remote systems are responsible for backing up and storing their data in a safe, secure location. The extent and frequency of the backup process is based on the business impact that would result from its loss.

A.4 Backup Procedures

Our backup information provides protection from almost any threat - accidental or deliberate, that could cause loss or destruction of data. A documented backup process must exist which defines the daily backup routines.

Backup techniques used must be capable of fully restoring all open/active files so that the integrity of these files is not compromised and that they can be fully restored to active operations.

All backup media must be labelled with the highest classification of the data that resides on the media.

All locally stored backup media must be kept in fire retardant media safes. Access must be limited to those who perform the backups. A log of the media in the safe must be maintained for use as a recovery aid.

Backup procedures must exist for handling daily backups as well as performing day to day restorations or full data recovery.

The backup process must be automated wherever possible in order to ensure consistency.

Randomly selected file restores must be performed at a minimum of monthly to ensure the readability of the backups (i.e. data is actually being written to tape) and to ensure that tape media is still readable.

Wherever feasible, backups must be verified by reading them back after they are written. Many backup software packages allow this to happen in conjunction with routine scheduled backups.

A.5 Off-Site Storage

Off-site information storage is defined as a secure off-campus location that is sufficiently distant from the primary location so that, in the event of a localised or area wide disaster, the backed up information will be safe and available for recovery.

The off-site location must have restricted access, yet be accessible when needed, at any time, night or day. If an outside company operates the location, it must be bonded and insured against loss or breach of security.

Off-site backup media must be given the same level of physical and environmental protection that are required for the primary site. This includes

security during the transporting of media and documentation between MCSB and the off-site location.

A documented procedure must be in place that outlines the off-site rotation process. At a minimum this must include a list of who is authorised to send data off-site, who is authorised to recall data, and who is authorised to make changes in access levels of MCSB employees.

A process must be in place for reviewing who has access to off-site processes. This review must be done at a minimum annually – or whenever there is a change in responsibilities that warrants it.

When off-site data is kept for multiple years, the media must be brought back and tested for integrity at a minimum annually. Data should be copied to new tapes at a frequency level which ensures data will not be lost per specifications of the type of media used. This must be performed more frequently when off-site data is extremely sensitive and is being kept for archival or legal purposes.

B. Disaster Recovery Planning Standards

Purpose

To state the MCSB Disaster Recovery Planning standards and responsibilities which are required for the protection of all business critical hardware, systems, applications and networks.

Scope

MCSB's essential business functions are highly dependent upon our computerized information systems. Natural (e.g. floods, storms, earthquakes) or man made (e.g. sabotage, operator error, equipment failures) disasters can terminate or severely disrupt business processing capabilities. Disaster Recovery Planning provides for the timely resumption of MCSB's essential business hardware, systems, applications and networks in the event of a disaster.

Responsibilities

Disaster Recovery Planning is a joint responsibility which is shared between "the custodians of the computer applications, equipment and facilities in co-ordination with the application system owners." Custodians are identified as the ones who are "responsible for the operation and maintenance of the data processing equipment." Systems owners are identified as the "user or group of users with the primary responsibility for updating the application files."

Because of this shared responsibility, someone must be selected to function as the Disaster Recovery Planning Co-ordinator. The Disaster Recovery Planning Co-ordinator will then work with the various areas in the development, testing and updating (maintaining) of the plan.

Disaster Recovery Planning Standards, includes the following subsections:

B.1 Identifying Critical Applications

B.2 Developing the Disaster Recovery Plan

B.3 Testing the Disaster Recovery Plan

B.4 Training

B.1 Identifying Critical Applications

The degree and scope of the Disaster Recovery Planning process is totally driven by the potential company and business impact that would result from the loss of a particular application, hardware, system, network and/or data. An application's business criticality is based on several evaluation areas.

Customer visibility measures the impact that the loss of the application would have from the perspective of MCSB customers (e.g. loss of customer or employee good will).

Financial impact evaluates the application's business importance in terms of how its loss would cause a loss of revenue, impact time to market or our inability to meet financial obligations.

The legal impact rates the application's business importance in terms of legal, contractual, governmental, or regulatory requirements.

The impact to the corporate image, which would result from the loss of an application and/or its data, is also evaluated. Such a loss could seriously erode our corporate reputation and shareholder confidence. A major loss could cause an inability to function as a company.

The methodology used to determine the criticality of business applications, systems, networks and/or data is the Business Impact Assessment (BIA) process. The BIA process is the most important step in Disaster Recovery Planning. In this phase, a business assessment is performed on each application running on the system or network being analysed. The result of this assessment determines the criticality of the application to the business and to MCSB as a whole. The criticality dictates how quickly the application needs to be recovered. This speed of recovery is then used to help design the proper recovery strategy. The BIA process also identifies how current the recovered data will need to be in order to return the business to an operational status.

It is through this process that the business recovery requirements are defined. These requirements then provide the design objectives for the data backup plan, recovery plan as well as the recovery time frame by which the effectiveness of the disaster recovery process will be measured.

A Business Impact Assessment (BIA) must be performed for each business application, data, system and/or network in order to establish the true level of business and data criticality.

The recovery timeframe must be reviewed, agreed upon by the affected business and Information Systems areas and documented. The criticality classification must be reviewed/updated by the system owner and equipment custodians:

When the application changes,
When significant changes in exposure occur, or at a minimum,
Annually.

Once the Business Impact has been determined, a Site-Risk Assessment must be performed to identify problems before they occur.

B.2 Developing a Disaster Recovery Plan

A Disaster Recovery Plan must contain all of the detailed steps, procedures and support information needed to recover the subject hardware, system, application and network in the event of a disaster.

A Disaster Recovery Co-ordinator must be assigned to co-ordinate the development, testing and updating (maintaining) of the plan.

Each system owner / equipment custodian must develop and document a Disaster Recovery Plan for each essential business application, system and/or network it supports.

Because of the sensitive nature of the material contained in the recovery plan, it must be classified as Confidential Proprietary.

Information Security procedures and mechanisms must be maintained during the recovery process. Each Disaster Recovery Plan must be reviewed using the Disaster Recovery Plan Review Check List. The plan must be tested and

updated yearly to reflect changes in the hardware, system, network and/or application.

A copy of the recovery plan, documentation and supplies must be kept in a secured off-site location.

B.3 Testing the Disaster Recovery Plan

It is impossible to overstate the importance and value received from testing the disaster recovery and back-up plan. Only through testing will any missing and/or critical pieces be identified that could have rendered the system UNRECOVERABLE. This section identifies the standards for testing a disaster recovery plan.

System owners and equipment custodians are responsible for testing their Disaster Recovery Plans at least once a year to ensure that the plans are accurate, complete and that the off-site data can be used to successfully recover the application. Where testing of the full plan is impractical, individual sections or sub-systems must be tested separately in order to confirm the recoverability of the plan as a whole.

The test recovery must be successfully completed with the hardware, system, network, application programs, data recovered and the applications functionally verified by the business or application support areas within the recovery time frame that was defined in the Business Impact Assessment process. Failed tests must be re-tested, within a timeframe that is agreeable to the business area, until completed successfully.

More frequent testing must be considered when a system, application and/or network has experienced a high degree of change. When performing the test, all materials, i.e. procedures, data, documentation, etc. needed to facilitate the recovery test must come from locations other than the primary processing site.

Where possible, personnel who are unfamiliar with the site being tested must be used to execute the recovery test in order to verify the detail and completeness of the recovery procedures.

A sequential log of test events must be kept which lists time frames, problems encountered and suggestions for improvement. This log must be expanded in a post mortem review and then used for problem tracking and resolution. The full test must be reviewed with the supported business(s).

B.4 Training

Training need to be provided for Disaster Recovery co-ordinators to ensure that they are aware of their responsibilities.

MCSB System Berhad

Computer Room Disaster Recovery Plan

(Draft Copy)

Table of Contents

1 Introduction

MCSB is an established organisation which depends highly on the use of computer –based systems to control and coordinate most of it's major operations. Due to this high level of dependency, it is absolutely essential that the necessary precautions are undertaken to ensure that the computer system remains accessible under every possible circumstance.

Therefore, in cases of unforseen disruptions to critical computing facilities, proper recovery or resumption procedures have to be devised and implemented to ensure that the impact on the major operations is minimized.

1.1 Using this plan

This plan is activated when an emergency occur, which is beyond the scope of standard operating procedures and remains in effect until operations are resumed at the primary site, or its replacement, and control is returned to appropriate functional management.

1.2 Objectives

The objective of the MCSB Disaster Recovery Plan is to provide a concise set of guidelines for key management, technical, and support staff in recovering MCSB's IT Infrastructure such as Computer Rooms, Systems and Network in the event of a disaster. The guidelines in this plan will outline all activities necessary to recover critical business applications identified herein.

A huge portion of the business units in MCSB depend on the uptime of the IT infrastructure for the success of MCSB's competitive edge. A proper guideline is tabulated with the intent of bringing up IT services to MCSB as quickly and efficiently as possible, and to allow all internal clients to resume back business activities.

1.3 Scope

This Disaster Recovery Plan scope refers only to corporate application and KL Office network, systems, applications hosted in MCSB Computer Rooms. Applications hosted in other MCSB sites are not covered in this plan.

1.4 Business Impact

In event of any disaster occurring in the site computer rooms, several systems and their respective applications will be impacted. The outage of the following systems can cause operations to be done and indirectly would cause services to customers halted. They are classified as Mission Critical (Class 1) and Critical (Class 2) with recovery time objective of less than 24 hours in the BIA.

Functional Areas	System ID	Description	Local Expertise	Application Support	Platform	Server Location	Users
Support	CIS	Customer Information System	H	MCSB	Unix	MCSB	RHD, SS
	Oracle	Oracle Development	H	MCSB	Unix	MCSB	Oracle
	FileServer	R&D Main Development	H	MCSB	W2000	MCSB	R&D

2 Disaster Declaration

2.1 Organization

Overview

The purpose of this section is to define Disaster Recovery Organization, the Escalation Plan and the roles and responsibilities of the Disaster recovery teams.

The full Disaster Recovery Team (DRT) includes technical experts and managers who work on smaller teams based on their area of support. Each team has a specific set of responsibilities. The teams are:

The description of ***"Crisis Management Team (CMT)"***
The description of ***"Disaster Recovery Team (DRT)"***

Crisis Management Team (CMT)

- *Consists of Managers and designated employees who forms the core team for the site crisis management.*
- *Review damage assessment report from Assessment Team to make the declaration decision, if necessary.*
- *Notify Executives of a potential disaster or threat at affected site.*
- *Declare Disaster with Recovery Site.*

- *Establish Crisis Center to coordinate the recovery efforts.*
- *Coordinate activities with the site crisis management team.*
- *Notify DR Coordinators to recall support teams, and begin the communication process with Executives and Customers.*
- *Coordinate management efforts to restore the processes, facilities, etc.*
- *Notify HR to handle any media questions.*

Disaster Recovery Team (DRT)

- *Conduct initial damage assessment of disaster area.*
- *Make recommendations on damage assessment to CMT*
- *Notify & mobilize the recovery team and support team members.*
- *Activate the recovery site, notifying the off-site tape storage location.*
- *Contact all vendor sources and customer engineers to order and install equipment and communication circuits.*
- *The Recovery Teams to restore all operating systems, program products, communications, and applications software required to utilize critical applications after the declaration of a disaster.*

2.2 Escalation

Upon an unscheduled outage, the on site personal will perform the initial assessment of the disaster and inform the IT DRP Coordinator and IT Manager. The cause of the outage can be due to natural disaster, system or electrical failure, fire, sabotage, or virus. For the purposes of this plan, a disaster is a situation or event that will result in the loss of hosting and communication capability to the MCSB for a continuous period of greater than 24 hours.

After the initial assessment, the IT DRP coordinator will inform the Crisis Management Team (CMT) on the impact of the disaster. Once the CMT has declared the outage as a disaster, the IT Disaster Recovery Team (DRT) will be notified.

Depending on the nature of the disaster, the specific execution of the disaster recovery plan will take place.

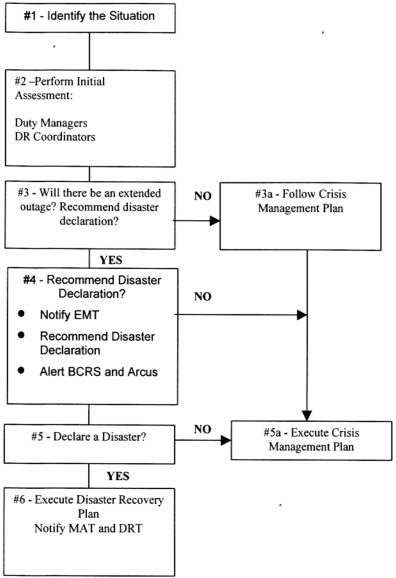
2.3 Team Contact List

The contact list for all the staffs are maintained in the DRP Master Contact List document

- *Crisis Management Team*

- *IT Disaster Recovery Team*
- *IT Support Team*
- *Network Contact Lists*
- *IT Vendor List*

Escalation Process Flow



Escalation – Action

#1 - Identify Situation

WHO EXECUTES: Onsite Personnel

Information Required:

Are personnel Safe?
What/when occurred, what equipment is effected?
What location(s) are effected; how can you be contacted?

 # 2 – Perform Initial Assessment

WHO EXECUTES: Onsite Personnel, Site Facilities
ACTION REQUIRED: Call the following:
Crisis Mgmt - 602-xxx-xxxx
Site Facilities - 602-xxx-xxxx
IT Systems Section Head /DRP Coordinator
IT Manager

#3 – Extended Outage?

WHO EXECUTES: ***IT DRP Coordinator***
ACTION REQUIRED:
1) *Determine if there will be an extended outage with the Initial Assessment Team,*

#4 – Review and Recommend Disaster Declaration

WHO EXECUTES: ***Initial Assessment Team – CMT Notification***
ACTION REQUIRED:
1) *Notify the Crisis Management Team (CMT)*
2) *Alert IT Disaster Recovery Team (DRT)*
3) *Provide them with the information gathered in Step #1.*

#5 – Declare a Disaster?

WHO EXECUTES: ***CMT Approval***
ACTION REQUIRED:
1) *Declare a disaster*

2) *Proceed with this recovery plan notifying recovery teams, recovery sites, and media recovery.*

3 Assessment

On notification by on site personnel on the disaster and evaluation of the Initial Assessment, the IT DRP coordinator will alert the IT Disaster Recovery Team and assemble the team to conduct a Damage Assessment.

3.1 Initial Assessment

The objective of the Initial Assessment is to gather information regarding the event and determine the areas affected. The on site (IT, Facilities or Security) personnel will perform the initial assessment of the event. The template below will guide the staff to collect the necessary initial information.

Table 3.1 Disaster Report Log

Initial Assessment	***Report***
What is the nature of the problem "event"?	
Who is reporting the problem	***NAME:*** ***DEPT:***
Where can they be reached?	*Tel Ext* *Handphone:*
When did the event happen?	*Time:*
Which areas are affected?	
Are you able to proceed to site?	
Are the premises safe to enter? If not, why.	
Are any people injured? Number of people and nature of injury.	

3.2 Damage Assessment

Damage Assessment Procedures:

The IT DRP Coordinator will notify and assemble the DRT. The DRT will determine the extend of the disaster and conduct damage assessment of the computing facility, equipment and business impact. The team will also determine recovery time and effort required.

*The **Disaster Recovery Team** assessment responsibilities include the following:*

1. *Responsibility for the overall damage assessment.*
2. *Assess damage to key computing equipment CPU's, DASD, Controllers, Tape Drive Units, Printers, telecommunications equipment, etc.) Prepare detailed lists of equipment that require repair or replacement and report status to the I/S Recovery Management Team.*
3. *Perform damage assessment of DASD recording media and tape libraries*
4. *Perform damage assessment to the operating system*
5. *Perform damage assessment to all critical system products*
6. *Establish contact with all vendor sources and service representatives for equipment for hardware order, shipment, and installation of new equipment.*
7. *Perform damage assessment of key structural assets (e.g., building, flooring, lighting, etc.).*
8. *Perform damage assessment of key main electrical systems (UPS main module power panel breakers, UPS by-pass, static switch, transfers, UPS generator, power distribution units, etc.)*
9. *Perform damage assessment to key HVAC systems (e.g., computer room, UPS, power distribution unit, etc.).*
10. *Provide for the general safety of other I/S Recovery Team members.*
11. *Perform damage assessment of key fire control systems (e.g., sprinklers, local and remote alarms, fire extinguishers, etc.). Establish contact with all vendor sources and customer engineers to begin the repair and rebuilding process of key facilities.*
12. *Establish and maintain Data Center security.*
13. *Prepare detailed lists of equipment that require repair or replacement for the I/S Recovery Management Team.*
14. *Report status to the Site Crisis Management Team*

*A summary of assessment tasks for the **Network Team** is outlined below. Damage assessment should be documented using the worksheets found in this section.*

1. *Perform damage assessment of all communications circuits*
2. *Perform damage assessment of all modems*
3. *Perform damage assessment of all front-end communications controller*
4. *Prepare detailed lists of circuits and communications equipment that requires repair or replacement for the Recovery Management Team.*
5. *Establish contact with all vendor sources and customer engineers for communications circuits and equipment for repair or ordering, receipt and install*
6. *Perform damage assessment of DASD recording media and tape libraries, Configure DASD, Processor Control Unit, channels, memory, and controllers as required.*
7. *Perform damage assessment to the operating system*
8. *Perform damage assessment to all critical system products*
9. *Report status to the Recovery Management Team*

3.3 Assessment Checklist

Table 3.2.1 Checklist for Main Computer Room

Computer Room	Equipment Name	Condition Good/Damaged	Recoverable?	Backup Available?
Main C.R.	Electrical/Fire/Gas/ Water			
Main C.R.	LAN Switches			
Main C.R.	MY1 WAN & Site Routers			
Main C.R.	NT Cluster Server (Windows services)			
Main C.R.	NT Server (QA Online)			
Main C.R.	Sun Server (Email)			

3.4 Assessment Report

The IT DRP team will produce an assessment report based on the damage assessment. Use the following guidelines to complete the assessment reports, based on the Damage Assessment done in Section 4.2 and the Business Impact in Section 1. This report must be completed and given to the Crisis Management Team to allow them to make decisions critical to the recovery of business operations.

TABLE 3.3.1 Assessment report

Equipment	Business Impact (Apps, System)	Repairable(R) or Salvageable(S) or Replaceable(P)?	Probable Recovery Time Frame (hrs)	Costs (RM$)

Total Hrs & Cost				

If time permits, provide a more detailed explanation here: (ex. implications, expectations, and limitations on recovery effort). This report should give the EMT the "feel" of recovery situation.

_____

_____

_____

_____

3.5 Action Plan

An Action Plan in response to the Assessment Report should be included here. Refer to Table 3.4.1 as a guide.

Table 3.4.1 Action Plans

Steps	***Action items***	***Responsibility***	***Date/Time***	***Status***	***Remark***

4 Recovery

This section documents the locations and activation procedures of pre-arranged recovery sites. The location selected will be determined by the extent of the damage. This recovery procedure cannot be applied in certain parts of the site. For the recovery of these areas, the Crisis Management Team will take over responsibility.

The primary duty of the Systems Recovery Team is to install and make operational all operating systems, program products, communications, and applications software required to restore critical applications within the hours specified by contractual agreement.

4.1 Recovery locations

The table below illustrates probable recovery locations for certain disaster areas.

Table 4.1 Recovery Locations

Disaster Area/ Application by List of Criticality	***Probable Recovery Site***	***Comments***
Main Computer Room	*MCSB PNG Computer Room*	
Unix Servers	*MCSB PNG Computer Room*	*WAN access*
NT Servers	*MCSB PNG Computer Room*	*WAN access*

4.2 Off Site Tape Storage

The back-up tape for systems residing in Site1 are kept in Safe Deposit Public Bank.

4.3 Administrator Passwords

Admin passwords for the systems are kept in seal envelopes and stored in the same location as the back-up tapes offsite storage.

4.4 Systems Disaster Recovery Plans.

All identified procedures critical for recovery are included with the individual disaster recovery plans stored in the off-site.

1. *Network Procedures*
2. *NT Procedures*
3. *UNIX Procedures*

5 Restoration

This section is effective when one of the 2 situations below exists:

1. *Decision is made to restore the disaster site.*
2. *Recovery site is operational, and the original site needs to be restored to allow business to resume its activities back in the site.*

5.1 System and Network Restoration and Recovery logistics

1. *Refer to the lists available in the Damage Assessment section in Chapter 3. Refer to Tables 3.3.1, which will identify all the damaged areas that needs to be worked on.*
2. *Refer to Table 3.4.1 for the full task breakdown, and personnel responsible to bring up the tasks*

5.2 Discontinuing the recovery site

Before proceeding to this section, System and Network Restoration as in Section 6.1 must be performed fully to ensure original site is up and running.

To discontinue the recovery site, perform the following steps:

1. *All workstations in the recovery site must be migrated back to the original site.*
2. *Start with the least critical systems first.*

3. *All systems at original site are back to their normal operation.*

4. *Shutdown all systems in the recovery site.*

5. *Transport all equipments back to the original site*

6 Review and Update Plan

Disaster Recovery plan is an ongoing, expanding process. Only through proper maintenance and testing will the plan stay current and viable.

The Disaster Recovery Plan and the individual Systems Disaster Recovery Plan are reviewed annually in June by the IT DRP Team. It will also be updated when necessary.

Other then the scheduled review process, the DRP document would also be updated if any the following changes:

- *Staff*
- *Applications*
- *System Software*
- *Procedures eg backup & recovery procedures*
- *Hardware*
- *Network*
- *Environment*

APPENDIX

Appendix 1 Master Contact List

A1.1 Crisis Management Team Numbers

This section contains contact numbers of all personnel that support the site, such as Site Services personnel, and Security personnel.

Area of responsibility	*Name*	***EXTN***	*Handphone*	*Home Number*
Facilities Manager	*KY*			
General Manager	*Sabri*			
IT Operations Manager	*Ather*			

A1.2 IT Disaster Recovery Team

This section contains names and contact number of the members of the IT Disaster Recovery Team. After assessment of the disaster, appropriate system recovery staffs would be pulled in depending on the nature of the disaster.

Area of Responsibility	*Name*	*Extn*	*Handphone*	***HOME NUMBER***
Data Center, Email	*William*			
Network	*Wilson*			
CIM Systems	*FC Lim*			
IT Management	*Sabri*			

A1.3 IT Support Personnel

This section contains names and contact number of all key people involved in the recovery of critical systems, such as the Tier III, System Administrators, Unix Administrators and Application Support.

Area of responsibility	*Name*	*Extn*	*Pager/ Handphone*	*Home Number*
Network	*Sabri*			
Computer Opns.	*Davi*			
NetBackup	*Alan*			
NT Servers	*Woo*			
ORACLE DBA	*Yap*			
Paging Center	*Electcoms*			

A1.4 Vendor/Supplier Contacts

Area of Responsibility	Company Name	Address	Contact	Number
HP Servers (CIM)	Hewlett Packar Malaysia S/B		Call Center (Office Hrs)	
			International Call Center	
			Soh Yong Seng	
			Terence	
Window and Sun Servers Servers	Computer System Adviser (CSA) S/B		Office	
			Call Cener	
			JH Wong	
Cisco Products	Wang-Global (M)	Wisma Tong Ah1, Jln PerakPO Box 1129950740 KL	Office	
			Fax	
			Call Cener	
			Lip Kok Sun	
			Teng Hock Chai	
Cisco Products	Cisco System (M) S/B	Level 9, Tower Block D Uptown 55 Jln SS21/39Damansara Uptown47400 PJ	Office	
			Fax	
			Call Cener	
			Paul Choy	
			Shaifuddin Shafie	
Cabletron Products	Cabletron (M Sdn Bhd	Lot 4.01 4th Floor, Menara Choy Fook On, No. 1B, Jln Yong Shook Lin, 46050 PJ	Office	
			Fax	
			Call Cener	
			Cho Loi Tat	
			Devan	
			P.Megat	
CI Worldcom				
Telekom Malaysia				

Appendix F: Risk Assessment

RISK ASSESSMENT PROCESS

EVALUATION WORKSHEET

ORGANIZATION _____

EVALUATED BY _____ DATE: ___/___/___

LOCATION _____

NO.	DESCRIPTION	Factor Rating (R) POOR	WEAK	FAIR	MARGINAL	QUALIFIED	OUTSTANDING	APPLICABILITY	SCORE
		0	2	4	6	8	10	(A)	(RxA)

1.1	Fire/Smoke Detection/Suppression: Is the area (*) equipped to detect and suppress smoke/fire?									
1.2	Water/Plumbing: Are all locations equipped to detect and drain water or any other liquid e.g., waste water, manufacturing chemicals, etc. in the event of flooding, leakage's, spillage's, etc.									
1.3	Climate Control: Is the climate control system(s) providing adequate cooling, humidity and filtration to the air in and around the LAN equipment?									
1.4	Power: Are mechanisms in place to provide adequate, continuous and "clean" power to the LAN/Servers?									
1.5	Physical Location: Are all LANs located in an area of the building free from potential hazards?									
1.6	Alarm System: Is the facility central alarm station continuously monitored?									
1.7	Physical Access: Are the LAN locations equipped to restrict/monitor entry and exit?									

(*) Location includes printer rooms, media library, backup storage area, telecommunications room, cooling units and associated supply/storage rooms.

(A) = The extent to which the criteria pertain to your environment (i.e., distributed clients and servers versus a mainframe LAN/Server area).

The applicability factor is generally the number 10 (i.e., applicable). If the criteria do not pertain to your environment , indicate this as a number between zero and nine and note why.