Disaster Recovery Plan

dd-mmm-yyyy

Government of xxx
Ministry of Education
Information & Communication Technology

INTRODUCTION

The Ministry of Education, maintains this written Disaster Recovery (DR) plan to minimize the effects of a disaster and allow MOE to quickly resume mission-critical functions. This disaster recovery plan serves to guide the MOE in the recovery and restoration of critical information technology systems in the event of a disaster assuming that the primary site is not recoverable for some time and as such ICT services need to be restored to a secondary survived site.

PLAN OVERVIEW

The disaster recovery plan is comprised of a number of sections that document resources and procedures to be used in the event that a disaster occurs and seriously impacts the MOE ICT systems. The plan includes requirements to perform the recovery tasks including roles and responsibilities of staff. The plan should be updated regularly based on changes to MOE computing and networking systems. Due to the very sensitive nature of the information contained in the full plan, it should be kept confidential and not published.

PURPOSE

The purpose of MOE DR plan is to prepare the MOE in the event of disruptions (e.g. natural disasters or man-made events). This plan will also guide restoration of ICT systems and operations to the widest extent possible in a minimum time frame. The plan encompasses all MOE office locations that are connected to the MOE network. The plan aims to minimize operational disruptions and to recover as rapidly as possible when an incident occurs. This plan identifies vulnerabilities and recommends necessary measures to prevent extended outages.

SCOPE

The scope of this plan is limited to provide a state of readiness allowing prompt response after a disaster has occurred. This, in turn, provides for a more effective and efficient recovery effort. This is a disaster recovery (DR) plan, not a daily problem resolution procedures document. See appendix for list of IT services that are included with the scope of the DR Plan.

PLAN OBJECTIVES

- Serves as a reference guide for MOE IT team

- Provides procedures and resources needed to assist in disaster recovery
- Identifies stakeholders that must be notified in the event of a disaster
- Assists in avoiding confusion experienced during a disaster by documenting, testing and reviewing disaster recovery procedures
- Identifies alternate resources
- Document the location of records and other relevant data

ASSUMPTIONS

- Key IT staff (Network Administrators, System Administrators etc) will be available following a disaster
- This plan and other critical network documents are stored in a secure off-site location and not only survived the disaster but are accessible immediately following a disaster
- The disaster recovery team is aware of their roles and responsibilities (see appendix)

DISASTER DEFINITION

Disasters can be the result of three broad categories of threats and hazards. The first category is natural hazards that include acts of nature such as floods, cyclones, earthquakes, volcano eruptions, tsunamis, fires, and landslides. The second category is technological hazards that include accidents or the failures of systems and structures such as water pipelines, utility disruptions and accidental hazardous material releases. The third category is human-caused threats that include intentional acts such as active assailant attacks, chemical or biological attacks, cyber-attacks / hacking against data or infrastructure, theft, viruses and sabotage. https://en.wikipedia.org/wiki/Disaster_recovery

PREPERATION

Initial assessment

In the event of a disaster, the IT Unit will conduct an initial damage assessment including the likelihood of a potentially prolonged outage and provide advice to the MOE senior management team on the estimate time to restore / recover all services. The MOE ITU may need to call vendors / providers to get estimates on the expected time to repair network services and / or replace equipment and the associated costs. An onsite inspection may not be possible if building access is not permitted based on the extent of the damage. The initial assessment should also include the following:

- Obtain information regarding damage to the primary data centre including physical structure, security, power and air conditioning
- Obtain information regarding damage to the ICT infrastructure assets including network, servers and storage
- Develop a restoration priority list to identify the facilities and equipment needed to resume operations
- Recommendations to resume operations

Disaster declaration

The MOE senior management team, with the initial assessment information provided by the IT Unit, is responsible for declaring a disaster and activating the disaster recovery plan.

Safety

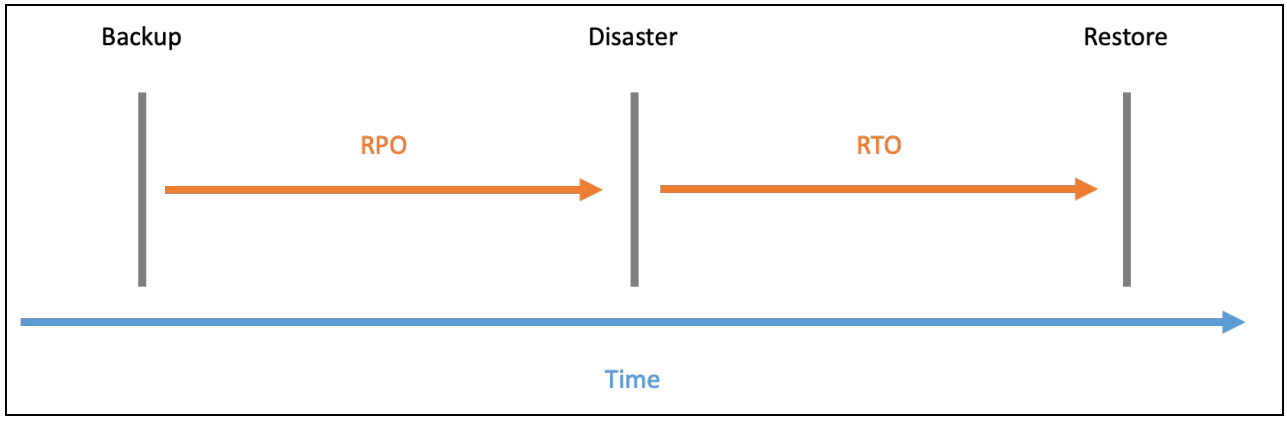
In the case of any disaster, the highest priority is the personal safety and protection of human life. As such, the site may need to be evacuated. It is important to prepare supplies including batteries, flashlights, first aid kit etc.

Recovery Time Objective

The Recovery Time Objective (RTO) is the targeted duration of time within which a service must be restored after a disaster in order to avoid unacceptable consequences. In other words, RTO is the acceptable amount of time that a MOE IT service can be offline.

Recovery Point Objective

A Recovery Point Objective (RPO) is the maximum targeted period during which data is lost from an IT service due to a major incident. In other words, RPO is the acceptable amount of time that MOE IT data can be permanently lost.



The diagram provides schematic representation of the terms RPO and RTO.

Recovery Time Actual (RTA)

The Recovery Time Actual (RTA) is the actual time taken to recover / restore services.

Backup / Secondary site

A backup / secondary site is a location where the MOE can relocate core IT systems in the event of a disaster. A backup, or alternate, or secondary site is the location of another data centre that is operated by the organisation or outsourced to another organisation. Backup sites are generally classified based on how prepared they are and the speed with which they can be brought into operation: "cold" (facility is prepared), "warm" (equipment is in place), "hot" (operational data is loaded) – with increasing cost to implement and maintain with increasing "temperature". https://en.wikipedia.org/wiki/Backup_site

Backup policy

Full and incremental backups protect and preserve critical MOE data and should be performed on a regular basis. Backup media should stored in a secure location that isolated from environmental hazards and geographically separate from the primary location.

- Backups greater than three years old are replaced.
- Backups fewer than *3* years old must be stored locally offsite.

Testing

The DR plan should be tested on an annual basis including timed rehearsals, during which the RTA gets determined and refined as needed. The test may be in the form of a walk-through, mock disaster, or component testing. The process of testing the DR Plan ensures that all services including associated components, authentication and access to data has been tested in advance of any disaster. Running practice tests ensures that the DR Plan is effective.

Updates

Considering the dynamic nature of the MOE environment, it is important to update the DR Plan regularly including technical information on systems and listing of personnel contact names and numbers. Technical diagrams may be attached to the DR Plan in the appendix as "quick references" when implementing the network DR plan or for testing purposes. Emergency contacts and home / mobile phone numbers of key stakeholders should be included in this document. The address of the primary and secondary data centre locations should also be

included in this document. The updated DR Plan should be printed and a hard-copy version of the DR Plan stored in the IT Unit in case the electronic version is not accessible from the MOE server during a disaster.

PROCEDURES

The following steps are recommended if there is enough advanced warning of a disaster such as a cyclone:

- Have multiple phones fully charged connected to different networks and / or satellite
- Verify that the backup generator is operational and has fuel
- Deploy portable generators on standby
- Notify technical personnel to be on standby
- Ensure that a vehicle is available
- Verify that system backups are up to date

Once an incident occurs it is important to notify all relevant stakeholders including:

- Emergency Services including ambulance, fire and police
- MOE Building Security
- MOE ITU Manager and staff
- MOE Management
- Other government ministries
- Power company
- Air conditioning service company
- Telecommunications company

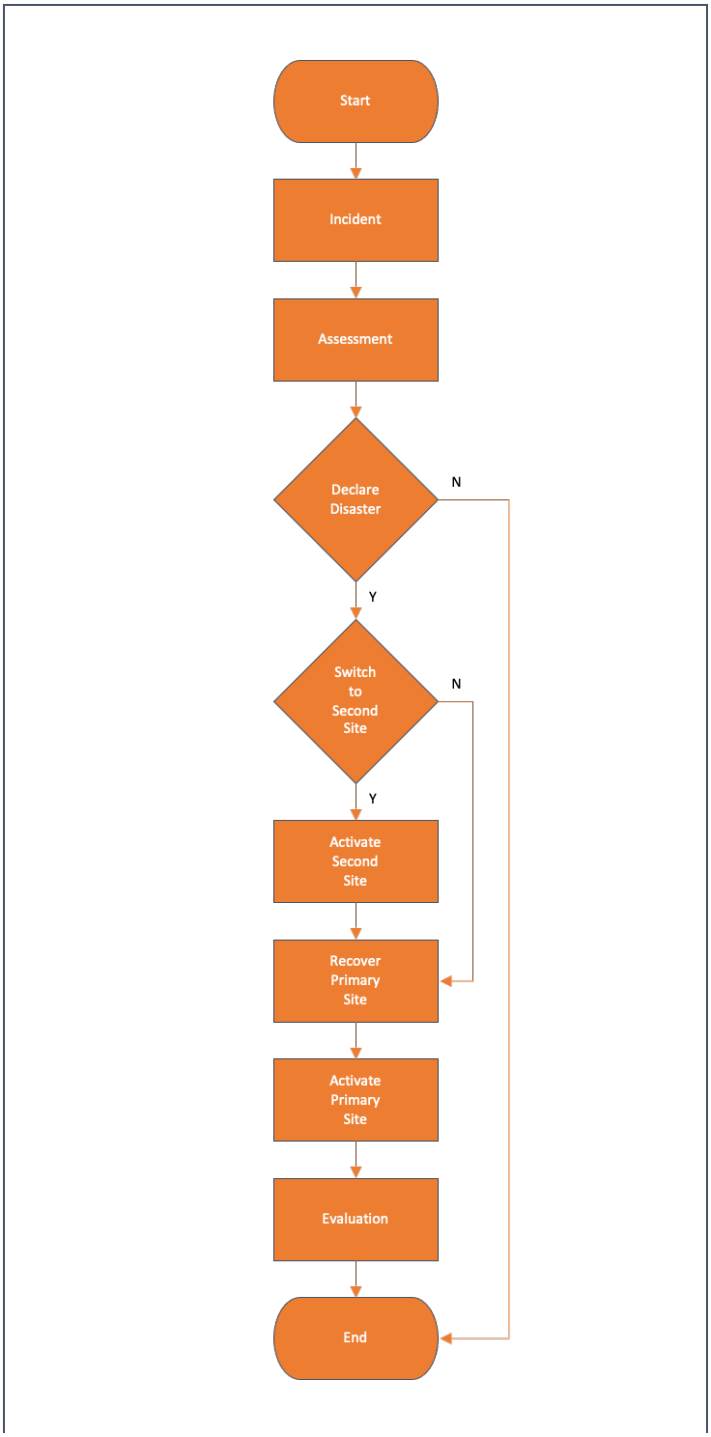
Official communications should be maintained through authorized government channels. These channels are designated as the principal contacts with the media (radio, television, and print), regulatory agency, government agencies and other external organizations following a formal disaster declaration.

In the case of a virus / hacking incident it is recommended to disconnect all services from the internet; whereas in the case of fire / water damage (burst / leaking pipe, cyclone / rain) it is recommended to power down all services; and in the case of a hardware / network incident it is recommended to contact the vendor.

The following procedures should be followed when an incident occurs:

1. An incident occurs and all relevant stakeholders are notified

2. MOE IT Unit conduct and initial assessment including time and cost of recovery
3. MOE Senior Management decide if a disaster should be declared
4. If a disaster is declared the MOE IT Unit will activate / switch over to the secondary site
5. MOE IT Unit will recover / reconstruct the primary site
6. MOE IT Unit will activate / switch over to the primary site
7. MOE IT Unit will conduction an evaluation of the process


Start
Incident
Assessment
Declare Disaster
N
Y
Switch to Second Site
N
Y
Activate Second Site
Recover Primary Site
Activate Primary Site
Evaluation
End

APPENDIX A: ROLES AND RESPONSIBILITIES

Charter:

The MOE IT Unit will be responsible for communications with senior management to determine a disaster declaration and then overall coordination of the disaster recovery effort, to facilitate recovery and restoration activities.

Responsibilities*:*

- Familiarize themselves with the contents of the disaster recovery plan
- Ensure that the disaster recovery plan is updated regularly
- Evaluates which recovery actions should be invoked
- Coordinate with the recovery team members and external stakeholders
- Analyze and assess damage
- Sets restoration priorities based on damage assessment
- Provides senior management with ongoing status information
- Sends out approved information to staff via agreed communication channels
- Work with external vendors including telecommunication carriers to develop a rebuild / repair schedule if required
- Establish command center
- Maintain a log of issues and actions
- Prepare post-disaster debriefing report
- Facilitate network recovery and restoration activities, providing guidance on replacement equipment, systems and network services, as required.
- Coordinate testing of IT systems to ensure that everything is functioning normally

APPENDIX B: CONTACTS

IT Unit

Organisation	Contact name	Address	Phone

Server and computer equipment suppliers

Organisation	Contact name	Address	Phone

Communications and network services suppliers

Organisation	Contact name	Address	Phone

APPENDIX C: LOCATIONS

Primary Site:

Secondary Site:

MOE Primary Site:

APPENDIX D: SERVICES

The following critical services are included in the scope of this DR plan

Service	Site	RTO
OpemEMIS Core	MOE	48 hours
OpenEMIS Data Warehouse	MOE	48 hours
OpenEMIS Portal	MOE	48 hours
OpenEMIS Dashboard	MOE	48 hours
OpenEMIS DataManager	MOE	48 hours
OpenEMIS Integrator	MOE	48 hours

The following critical services are NOT included in the scope of this DR plan

Service	Site	RTO

APPENDIX E: INCIDENT FORM

This document will be used to log and update issues.

Date:		**Time:**	
Reporter First Name:		**Reporter Last Name:**	
Reporter Phone		**Reporter Email:**	
Reporter Department:		**Reporter Location:**	
Priority:	Blocker Critical Major Minor Trivial	**Type:**	General Hardware Software Network System
Summary			
When (Date / Time)	**Who (IT Officer)**	**What (Comments / Actions)**	
When (Date / Time)	**Who (IT Officer)**	**What (Comments / Actions)**	
When (Date / Time)	**Who (IT Officer)**	**What (Comments / Actions)**	
When (Date / Time)	**Who (IT Support)**	**What (Comments / Actions)**	

APPENDIX F: WIDE AREA NETWORK ARCHITECURE