Draft ICT Disaster Recovery Plan

Version	3.0
Draft Date	June 2014
Status	Draft
Approved By:	

Table of Contents

1.0 Introduction

Mbarara University of Science and Technology started in 1989 with 43 students in the Faculty of Medicine. Currently the university boosts of 3,500 students in the 3 Faculties of: Faculty of Medicine, Science and Development Studies; and Institute of Computer Science. Coupled with growth in enrolment, the university continues to increase its reliance on Computer and Network based systems to improve the efficiency and effectiveness of its day-to-day business processes. Considerable efforts have been made at digitizing the Academic Registrar's Department, the library, the Dean of Students Department, together with the existing web services which include university web page, staff mail, student mail and an e-learning portal. This is in addition to the official information stored by both staff and students as they work on their respective desktop or laptop computers.

At the centre of all these applications and services is the data processed and stored by the systems. This data is very crucial and must be kept safe in such a way that any possible scenario may not lead to loss and subsequent repercussions to the business processes in place. Currently, there is no central storage facility and disaster recovery plan. Computer system users individually store their data and information with very minimal safeguard controls in place.

It should be noted that despite MUST's advancements in Information and Communications Technology, there still exists several risk factors, that could result into the worst catastrophic disasters of permanent loss of any data or information stored over a period of reliance on the use of Computer and Network based Systems.

The primary aim of this Data Recovery Plan is to provide an action plan in response to a disaster that destroys the university's central computer systems run by the Computing Services Unit/Department located in the Main Data Centre in the Institute of Computer Science Block.

It is however important to note that, this plan does not guarantee zero data loss in the event of a computer system related disaster at Mbarara University of Science and Technology.

1.1 Objectives of the Disaster Recovery Policy/plan

- To develop orderly course of action for restoring critical computing capability within the shortest possible time after the occurrence of a disaster.
- Outline criteria for making decisions to recover and repair data and equipment hosted in the university's data centre.
- Provide information about personnel and technical expertise required.
- Identify equipment and facilities necessary for recovery.
- Ensure full restoration of facility

2. 0 Disaster Planning

2.1 Risks and Prevention

The Disaster planning process at Mbarara University should start by evaluating the risks currently existent at the University's Data Centre which could spark off a disaster, as highlighted below:

2.1.1 Electricity related damages to Equipment and Data

The greatest risk at Mbarara University is the inconsistent and ever fluctuating electricity supply to the data centre, through the national electricity grid. This can have severe effects of shortening the lifespan of the equipment and completely destroying the data stored on the storage media attached.

Preventive Measures

- The danger posed by the erratic nature of the electricity supply can be reduced by installing power back up systems to run for at least 10 hours in all designated data centers and server rooms at the university.
- The Computing Services Unit/Dept. shall implement a centralized data storage solution for all university data and information.
- The Computing Services Unit/Dept shall implement both real time and regular back up procedures of data hosted at all designated data centers in the university.

2.1.2 Fire

The amount of electricity supplied to the university's main data center, the several electrical connections and fluctuating power supply could at anytime result in short circuits. Short circuits are known to be very common causes of fire outbreaks, which could destroy the equipment and data stored in the data center.

Preventive Measures

- Installation of fire and smoke detectors in the data centre.
- Installation of hand-held fire extinguishers in visible locations, throughout the building.
- Staff shall be required to undergo training on the proper fire fighting to take in the event of a fire.
- Periodic inspection of the facility by University Electricians at least thrice a year, to eliminate any possible short circuits that may cause fires.

2.1.3 Flooding and Leakages

The current data center faces the risk of water leakages emanating from the air-conditioning units installed there-in.

There is also the possibility of flooding resulting from rain water over flow, from the windows of the facility.

Preventive Measures

- Periodic service maintenance shall have to be done for the air-conditioning units in the facility, in order to avert the occurrence of water leakages
- Periodic inspection of the facility by the University Estates and Works Department, to eliminate any possible causes of flooding and leakages.

2.1.4 Lightning

There is always the looming risk of a lightning bolt striking in this part of the world. If this struck it could result into the permanent damage of the equipment within the data center.

Preventive Measures

- Lightening Arresters shall be installed and maintained on the roof of the building housing the data center.

2.1.5 Computer Crime /Hacking

Computer related crimes like hacking are on the increase in the country and world over. The systems at Mbarara University would be an obvious target for hackers and crackers. This unauthorized access to the system could lead to the tampering or damage to the data hosted by the systems.

Preventive Measures

- The Computing Services Unit shall implement both software and hardware security controls to avert any hacking attempt into the university's computer and network systems e.g. Firewalls, Access Control lists etc

2.1.6 Theft, Terrorism and Sabotage

The university's data center may be physically accessed by unauthorized persons to carry out acts of theft, terrorism or sabotage. This could lead to destruction or the compromising of the data hosted in the facility.

Preventive Measures

- The university's security office shall increase the vigilance of patrols around the facility, especially during the nights.
- The door to the datacenter should always be securely locked and access keys only issued to authorized personnel.
- Adequate lighting shall be provided around the facility during the nights.

3.0 Disaster Preparation

3.1 Replication facilities

The university shall set up a number of replication facilities (hot sites) to mirror all the data hosted in the main data center. Any of these sites will automatically be the temporal main hosting site in case a disaster befell the main data center, before the facilities in the main data center are restored.

The following options shall be considered in choosing the alternate replication facilities.

- Setting up a hot site data center within the university campus in the New Science Block.
- Setting up a Warm site data center at the university's proposed Kihumuro Campus
- Set up a Warm site data center with a hosting company at a cost.

3.2 Replacement Equipment

In case of any disaster there shall be a sizeable amount of equipment, lost that will have to be replaced in order for the facility to be restored.
The following shall therefore have to be in place:

- Preparation of a complete inventory of all the components of each computer and network system and their software that must be restored after a disaster by the Computing Services Unit.
- Provisions within the University's Procurement procedure to allow for emergency procurement situations like disasters.
- Prequalified suppliers/service providers to provide replacement equipment in case of disaster.

3.3 Backups

The greatest insurance to computer data loss is making regular backups of the original data.
The Computing Services Unit shall therefore implement backup processes on external hard drive infrastructure for all university data and information in the following ways;

- Real-time data backup within the main data center.
- Real-time data backup of the site in the New Science Block.
- Periodic data backup of the site at Kihumuro
- Periodic data backup of the site at the Hosting Company.

3.4 Backup Procedure

Every Application system running within the university shall define and implement both automatic and scheduled back up procedures, in line with the available facilities, hardware and software.

The Developers of the application systems shall clearly provide functionality for back up within the system and clearly indicate this in the documentation.

4.0 Initiation of Emergency Procedures

4.1 Disaster Notification List

In the event that a disaster actually occurs there is a need for a list of important players to be notified immediately. The list shall be compiled and clearly displayed in case of any eventuality.

- University Security Office
- Uganda Police
- Fire Brigade
- Ambulance/Hospital Services
- Computing Services Unit/Department Staff Contacts
- Deans/Directors of Faculties and Institutes
- University Secretary
- Vice Chancellor

4.2 Disaster Recovery Team

The Disaster Recovery Team shall be tasked with the responsibility of ensuring that all university systems, applications, data and information are restored for user access in the shortest possible time following the occurrence of a disaster.
The team will suitably be headed by the Head of Computing Services and composed of all Systems, Web and Network Administrators and IT Officers.

4.2.1 Activating the Disaster Recovery Plan

The greatest aim of the operation shall be to restore all systems functionality with no data loss. The following describes a series of actions to be performed after a disaster has occurred;

- Recovery Manager shall appoint a Recovery Management Team, in consultation with all university stakeholders.
- Recovery Manager convenes a meeting of the Recovery Management Team.
- Each member’s responsibility in the recovery shall be reviewed.

- Recovery manager shall review the recovery plan with the recovery team.
- Each member shall perform their respective responsibility.
- Next meeting of recovery team shall be scheduled.

5.0 Equipment Protection

5.1 Protection

During the recovery process any equipment, magnetic media and other items damaged at the site shall be protected from any elements to avoid further damage.

5.2 Inventory

As soon as practicable, a complete inventory of all salvageable equipment shall be taken along with estimates about when the equipment will be ready for use and the list of items to be freshly procured.

5.3 Damage Assessment

There shall be a preliminary damage assessment intended to establish the extent of damage to critical hardware and the facility that houses it to determine what should be procured immediately.

5.4 Emergency Procurement

Having fully established the equipment to be replaced, emergency procurement procedures shall be initiated for this equipment to be replaced as soon as practicable.

6.0 Initiation of Recovery Procedures

Once the occurrence of a disaster results into the non-functioning of any application system or retrieval/access of information at the main data center, then any one of the replication sites referred to in section 3.1 shall be temporarily lit up to act as the main data center for the entire recovery process.

The choice of which site to use shall depend on an evaluation by the Recovery team on which site is adequately prepared to take up the immediate role of hosting all data processes.

6.1 Site Preparation

Having fully re-directed the central data processing activity to one of the replication sites, the recovery team shall embark on recovering the primary computing and network facilities. A process that shall be highly dependent on how quickly replacement equipment can be procured.

6.2 System Platform Recovery Procedures

The Recovery shall thereafter recover and restore all university systems and run the restoration of the data backups of these systems

6.3 Critical Applications

Throughout the recovery and restoration process, the recovery team shall decide which systems are critical enough to take precedence of others.

6.4 Restoration of the Data center

Once all the restoration procedures have been performed and reviewed, the main data center shall undergo rigorous tests before it is re-established as the main datacenter and the others act as replication sites.

7.0 Maintaining the Disaster Recovery Plan

In-order for this Disaster Recovery Plan to be maintained, it shall be made available to all relevant stakeholders.

This plan shall also be reviewed at least once a year by the university's ICT Committee.

It is important to note that since the university's computing infrastructure continues to change, the plan shall therefore have to change accordingly.