MUHIMBILI UNIVERSITY OF HEALTH AND ALLIED SCIENCES

ICT DISASTER RECOVERY PLAN (DRP)

VERSION 1.0

November, 2017

Table of Contents

ACRONYMS

DCIS	Dental Clinic Information System
DNS	Domain Names System
DR	Disaster Recovery
DRMT	Disaster Recovery Management Team
DRP	Disaster Recovery Plan
HIMS	Hospital Information Management System
ICT	Information and Communication Technology
LAN	Local Area Network
MAMC	MUHAS Academic Medical Centre
MUHAS	Muhimbili University of Health and Allied Sciences
PACS	Picture Archival and Communication System
RTO	Recovery Time Objectives
SARIS	Student Academic Information System
VOIP	Voice Over Internet Protocol
WAN	Wide Area Network

1 INTRODUCTION

Muhimbili University of Health and Allied Sciences (MUHAS) Information and Communication Technology (ICT) Policy requires the Directorate of Information and Communication Technology (DICT) to maintain a written disaster recovery plan that addresses information resources so that the effects of a disaster will be minimized and the institution will be able to either maintain or quickly resume mission-critical functions. This is due to the fact that staff and students of the University all rely heavily on the ICT infrastructure and services to accomplish their work and as an integral part of the teaching, learning, research and services environment.

As a result of this reliance, ICT services are considered a critical component in the daily operations of the University, requiring a comprehensive Disaster Recovery Plan to assure that these services can be re-established quickly and completely in the event of a disaster of any magnitude. Response to and recovery from a disaster at MUHAS is managed by an ICT Disaster Recovery Management Team (DRMT).

Definition of Disaster

"For the purposes of this plan a Disaster is defined as loss or damage of part or all of the University's ICT Infrastructure, which would have a high, or very high, business impact on the University."

Disaster, as outlined in the above definition, includes:

a) Total loss of one site, (i.e. due to fire damage)
b) Loss or technical failure of one or more network servers
c) Loss or technical failure of network infrastructure i.e. hub/switch/router/commas link
d) Loss or technical failure or Voice Infrastructure, (telephone system)
e) Extended loss of electrical power
f) Failure of a key software system

2 Purpose

This Disaster Recovery Plan (DRP) serves as the guide for MUHAS Information and Communication Technology (ICT) Services management and staff in the recovery and restoration

of the information and communication technology systems and services in the event that a disaster occurs, with the fundamental goal of allowing basic business functions to resume and continue until such time as all systems can be restored to pre-disaster functionality. This includes:

a) Preventing the loss of the organization's resources such as physical ICT assets, software and data/information
b) Minimizing downtime related to ICT
c) Keeping the business running in the event of a disaster

3 Scope

The MUHAS ICT DRP takes all of the following areas into consideration:

a) Network Infrastructure
b) Servers Infrastructure
c) Telephone System
d) Data Storage and Backup Systems
e) Data Output Devices
f) End-user Computers
g) Organizational Software Systems
h) Database Systems
i) ICT Documentation

This DRP does not take into consideration any non-ICT, personnel/Human Resources and real estate related disasters. For any disasters that are not addressed in this document, they should be covered in the business continuity plan of the University.

4 Version Information & Changes

This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, the plan should be treated as a confidential document. Any changes, edits and updates made to the DRP will be recorded in the template provided in Table 1. It is the responsibility of the ICT Disaster Recovery and Managment Coordinator to ensure that all existing copies of the DRP are up to date. Whenever

there is an update to the DRP, the University requires that the version number be updated to indicate this.

Table 1: Changes in DR Plan

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
DICT	*DR Coordinator*	*17/10/2017*	*1.0*	*Initial revised version of DR Plan*

Official copies of the document are available at the following locations:

- Office of DVC-ARC
- Office of Director of Information and Communication Technology

5 Plan Activation

This plan will be activated in response to internal or external threats to the Information and Communication Technology Infrastructure and systems of MUHAS. Internal threats could include fire, bomb threat, and loss of power or other utility or other incidents that threaten ICT facilities and services. External threats include events that put the ICT facilities in danger. Examples might include severe weather or a disruptive incident in the community. Once a threat has been confirmed, the ICT disaster recovery plan management team will assess the situation and initiate the plan if necessary.

6 Plan Overview

The disaster recovery plan (DRP) is composed of a number of sections that document resources and procedures to be used in the event that a disaster occurs at the Information Technology Services data centre located in the University. Each supported application or platform has a

section containing specific recovery procedures. There are also sections that document the personnel that will be needed to perform the recovery tasks named DISASTER RECOVERY ELEMENTS AND ANTICIPATIONS.

MUHAS has ICT infrastructure, a set of IT services, several IT service processes and a shared IT service center managed by Directorate of ICT. These systems and IT Equipment (described further in section 2.1 – section 2.5) need to be protected so as to ensure services are not disrupted in the event of disaster. In additional, the maximum targeted periods by which data recovery or service resumption can be tolerated are as indicated in Section 2.6.

6.1Current Network Architecture

The current network architecture is provided in Appendix 1.

6.2ICT SYSTEMS

The current list of all ICT Systems at MUHAS is provided in Appendix 2.

6.3CONNECTIVITY

Table 2: MUHAS Internet Connectivity details

Provider	Circuit Type	Bandwidth	Address	Onsite Location	Notes
COSTECH/TERNET (HEREIN) via TTCL	Optic Fiber	40Mbps	Tanzania Education and Research Network(TERNET) P.O. Box 95062, Ali Hassan Mwinyi Road, Kijitonyama (Sayansi) COSTECH Building, Dar es Salaam, Tanzania, Email: helpdesk@ternet.or.tz Tel:+255222775378	Main link at Muhimbili Campus	Terminated at MPL Building server room
Raha Liquid Telecom	Optic Fiber	30Mbps	8th / 9th Floor, I.T. Plaza Ohio St. /Garden Avenue, Dar-es-Salaam, Tanzania +255 222125230 +255 688 111222, info@raha.co.tz	Back up link at Muhimbili Campus	Terminated at MPL Building server room
TTCL	Optic Fiber	20Mbps	Tanzania Telecommunications Company Ltd. Extelcoms House, Samora Avenue P. O. Box 9070, Dar es salaam. Telephone: +255 22 214 2000 FAX: +255 22 214 2045 E-mail: info@ttcl.co.tz	Main Link at MAMC, Mloganzila	Terminated at Ground Floor, MAMC at Mloganzila campus

Provider	Circuit Type	Bandwidth	Address	Onsite Location	Notes
TTCL	VSAT	5Mbps	Tanzania Telecommunications Company Ltd. Extelcoms House, Samora Avenue P. O. Box 9070, Dar es salaam. Telephone: +255 22 214 2000 FAX: +255 22 214 2045 E-mail: info@ttcl.co.tz	Backup Link at MAMC	Terminated at Roof of MAMC at Mloganzila campus

6.4NETWORK EQUIPMENT

SWITCHES

(a) MUHAS Network Switches details (MAIN CAMPUS) is provided in appendix 4

(b) MUHAS Network Access Point details (MAIN CAMPUS) is provided in appendix 5

(c) MUHAS Network Switches details (at MAMC) is provided in appendix 6

(d) MUHAS Network Access Point details (at MAMC) is provided in appendix 7

ROUTER

Table 3: List of Available Routers

Make/Model	Description	IP	Misc. Details
Cisco 2941 Router	Gateway for MUHAS network	192.168.0.3	Gateway for MUHAS network
Cisco 3925 Router	Gateway for MAMC network	10.1.1.1	Gateway for MAMC network

FIREWALLS

Table 4: List of Available Firewalls

Make/Model	Description	M IP	Notes
CISCO ASA 5520	Cisco ASA 5500 Series Adaptive Security Appliances	192.168.0.150	At Muhimbili campus
PfSense 2.3.4-RELEASE-p1	Open Source Firewall and Router	192.168.0.78	At Muhimbili campus
Juniper SRX240H2	Firewall Security Appliance	172.16.98.1	At MAMC

6.5 SERVERS

The following are the available physical and virtual at MUHAS arranged in their order of criticality or important.

Table 5: List of available servers

Name	Rank	VM or PHY	Type/Make/Model	CPU	RAM	Disk	OS Version	Purpose
Epicor9 Server	1	VM	NA	2.8GHz (2 processors)	70 GB		Windows Server 2008 R2 Enterprise	Financial Management Software
SARIS 1	1	Physical Server	HP Proliant DL380 GS	2.0 GHz (2 processors)	2GB	250GB	Ubuntu 10.04.4 LTS	Keeping Student Academic Records
SARIS 2	1	VM	NA	2.4 GHz (2 processors)	8GB		Debian 9.0.0	Online Application/ Student Academic Records
SARIS TEST	2	VM	NA	2.0 GHz (2 processors)	8GB		Debian 9.0.0	Online Application/ Student Academic Records
Moodle (Elearing)	2	VM	NA	2.0 GHz (2 processors)	6GB		CentOS 7.0	Learning Management Systems
Zimbra Mail server (Community Edition)	1	Physical Server	Dell PowerEdge R620	2.4 GHz (2 processors)	32GB	6TB	CentOS 7	MUHAS Mail communications
Koha Integrated Library System	2	VM	NA	2.0 GHz (2 processors)	2GB		Ubuntu 16.04 LTS	Integrated Library Management Systems
Open Journal System	3	VM	NA	2.4 GHz (2 processors)	2GB		CentOS 6.8	

Name	Rank	VM or PHY	Type/Make/Model	CPU	RAM	Disk	OS Version	Purpose
Dspace repository software	1	VM	NA	2.0 GHz (2 processors)	2GB		Ubuntu 16.04 LTS	Repository
ownCloud	2	Physical	Dell PowerEdge NX3200	2.4 GHz (2 processors)	32GB	10 TB	CentOS 7	File storage and sharing
Conference System - open conference	3	VM	NA		2GB		CentOS 6.8	Scientific Conferencing System
Webserver Node 1	1	VM	NA		2GB		CentOS 7.0	Web Server
Webserver Node 2	2	VM	NA		2GB		Ubuntu 14.04.3 LTS	Web Server
Web server Node 3	1	VM	NA		2GB		CentOS 5.11	Web Server
DNS Server 1	1	VM	NA		2GB		CentOS 7	For DNS services
DNS Server 1	1	VM	NA		2GB		CentOS 7	For DNS services
DHCP Server	1	VM	NA		2GB		CentOS 7	For DHCP services
Dental Management Information System (Dentrix)	1	Physical			16GB		Windows Server 2008	Dental Management Software
NHIF Claim	1	Physical			4GB			NHIF claim

Name	Rank	VM or PHY	Type/Make/Model	CPU	RAM	Disk	OS Version	Purpose
Management System								management system
eTicket Tracking System (OTRS)	2	VM	NA		2GB		CentOS 7	Online Ticketing
Redcap	2	VM	NA		2GB		CentOS 7	Research Systems
Documentation Server	2	VM	NA		3GB		CentOS 7	Documentation Systems
Proxy Server 1	1	VM	NA		2GB		CentOS 7	Proxy Services
Proxy Server 71	2	VM	NA		2GB		CentOS 7	Proxy Services
Proxy Server 72	2	VM	NA		2GB		CentOS 7	Proxy Services
Proxy Server 73	2	VM	NA		2GB		CentOS 7	Proxy Services
Main HMIS &PACS server	1	Physical			16GB	8TB	Windows server 2012R2 Standards	Hospital Management Information Systems
Standby HMIS & PACS Server	1	Physical			16GB	8TB	Windows server 2012R2 Standards	HIMS
Domain Controller and NMS Server	1	Physical			32GB	2TB	Windows server 2012R2 Standards	Active Directory
EPICOR Server (Active)	2	Physical			16GB	4TB	Windows server 2012R2 Standards	Financial Management Software
EPICOR Server (Stand by)	2	Physical			16GB	4TB	Windows server 2012R2 Standards	Financial Management Software
HIMS training Server	2	Physical			4TB	2TB	Windows server 2012R2 Standards	HIMS Testing and Training
Biometric	3	VM	NA		1GB	1GB	Windows server	BVR system

Name	Rank	VM or PHY	Type/Make/Model	CPU	RAM	Disk	OS Version	Purpose
and Time Attendance System							2012R2 Standards	
Fire Alarm Server	1	Physical			4GB		Windows 7 64 bits	Fire System
Access Control Server	1	Physical			12GB		Windows 8.1 64 bits	Access Control System
Public Addressing server	1	Physical			12GB		Windows 8.1 64 bits	Public Addressing System

Note: (Rank of "1" = most important)

7 RECOVERY ANTICIPATION OBJECTIVES AND PRIORITIES

Currently, MUHAS has three Data Centres (Server Rooms), two at Muhimbili campus and one at MAMC, Mloganzila campus. The mission critical services/systems are being backed up at each data centre to ensure availability of data and services when disaster occurs. The Section defines the Recovery Time Objective (RTO) which is the targeted duration of time and a service level within which MUHAS business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in provision of services. In addition, the plan defines Recovery Point Objective (RPO) defines the maximum targeted period in which data might be lost from an available service due to a major incident. The Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are one of the most important parameters of a disaster recovery or data protection plan within MUHAS. These objectives guide the University to choose an optimal data backup (rather restore) plan

It needs to be noted that different authorities have set up categories of RPO and RTO. The Computer Network Technologies (CNT) has developed a scheme by categorizing RTOs and RPOs into different classes. Class 1 is the lowest level, where acceptable recovery times range from 72 hours to one week, and the most up-to-date data can be from a weekly backup. A class 4 recovery environment contains the most stringent requirements. With Class 4, the recovery time must be immediate and the data recovered must be less than one second old. The following table illustrates this Recovery Classes 4-tier scheme:

Table 6: General Recovery Schemes

	Class 1	**Class 2**	**Class 3**	**Class 4**
RTO	72 Hours - 1 Week	8 - 72 Hours	Less than 8 Hours	0 Minutes
RPO	Last full backup - Less than 1 Wk	Last Backup - less than 24 Hrs	Less than 15 Min. before the Event	0 Minutes

7.1RECOVERY TIME OBJECTIVE (RTO)

Generally, the recommended RTO's based on Setup and Configuration of MUHAS

infrastructure is of Class 2 whereby recovery times should be within 8 - 72 Hours. The specific RTO's is as indicated in Table 7.

Table 7: The Recovery Time Objectives

SERVICE /APPLICATION	RECOVERY OBJECTIVE
LAN (Local Area Network)	3 days estimate
WAN (Wide Area Network)	3 days estimate
Internet	Within 30 minutes after LAN/WAN restored
Applications	1 day Estimate (*The duration might vary per application Priority Level indicated in Section 2.6.3*)

These RTO's should be considered best-case estimates. Currently, MUHAS does not have computer hardware available for recovery nor contracts or agreements in place to obtain hardware on a priority basis. In the event of a disaster, hardware would have to be located, purchased, shipped, installed, and configured before any software or data could be installed or restored. The availability of the relevant equipment and shipping times could vary greatly depending on the timing and scope of the disaster.

The network services and application recovery times are additive in case of a disaster that affects servers and the LAN. However, a WAN disaster takes significantly longer to recover from due to the installation schedules of internet service providers (ISP). During this delay, server and LAN recovery could be completed so the WAN recovery time would be the only time applicable to the RTO.

7.2 RECOVERY POINT OBJECTIVE (RPO)

Generally, the recommended RPO's based on Setup and Configuration of MUHAS infrastructure is of Class 2 whereby recovery points should be of less than 24 hours. However, this might vary depending of criticality of data and/or priority of Service. The Application Recovery Priories are indicated in Section 2.6.3.

7.3APPLICATION RECOVERY PRIORITIES

MUHAS's applications are identified and classified below in priority order. Depending on when the disaster takes place, these priorities may change. The inventory of the systems and their priority within the below classification level are as indicated in Table 8 – Table 10. The definition of Tier levels is as follows: -

- Tier 1 - Critical Systems
- Tier 2 – 2nd level systems, moderate impact
- Tier 3 – 3rd level systems, low impact

Tier 1 Priority Applications

Table 8: List of Tier 1 Applications

Application	**Host Location**
Public DNS, DHCP Server	MPL Data Center
EPICOR IFMIS	MPL Data Center
Email Server	MPL Data Center
Hyper-V Hosts (2 Citrix Xen Servers)	MPL Data Center
Web Server (Main)	MPL Data Center
HIMS (HIS, PACS)	MAMC Data Center
DENTRIX/DEXIS	Dental School Server Room
SARIS	MPL Data Center

Tier 2 Priority Applications

Table 9: List of Tier 2 Applications

Application	**Data Communication Method to Disaster Recovery Site**
Proxy Server	Backups stored at HD-CHPE/MAMC
Web Server (Backup)	Backups stored at HD-CHPE/MAMC
E-Learning (Main)	Backups stored at HD-CHPE/MAMC

Tier 3 Priority Applications

Table 9: List of Tier 3 Applications

Application	**Data Communication Method to Disaster Recovery Site**
E-Learning (Demo)	Backups stored at HD-CHPE/MAMC
Core Switch (Main Distribution)	Backups stored at HD-CHPE/MAMC
Active Directory	Backups stored at HD-CHPE/MAMC
Hyper-V Hosts (VMware Sphere)	Backups stored at HD-CHPE/MAMC

8 COMMUNICATING DURING A DISASTER

In the event of a disaster the University will need to communicate with staff, students and other key shareholders to inform them of the effects on the business, surrounding areas and timelines. DICT or other designated officer will be responsible for contacting all of MUHAS's stakeholders.

8.1 Communicating with the University Management

DICT's first priority will be to ensure that the University Management, Key Departments and other Key Authorities have been notified of the disaster, providing the following information:

a) The location of the disaster
b) The nature of the disaster
c) The magnitude of the disaster
d) The impact of the disaster
e) Assistance required in overcoming the disaster
f) Anticipated timelines

Authorities Contacts

Authorities	Point of Contact	Phone Number	E-mail
University Management	DVC PFA	<<Phone Number>>	dvcpfa@muhas.ac.tz
Auxiliary Police	<<Contact Name>>	<<Phone Number>>	<<Contact E-mail>>
Police Force	<<Contact Name>>	<<Phone Number>>	<<Contact E-mail>>
Fire and Rescue Force	Hotline	112	info@.....

8.2Communicating with Employees

DICT's second priority will be to ensure that the entire University has been notified of the disaster. The best and/or most practical means of contacting all of the employees will be used with preference on the following methods (in order):

a) E-mail (via University e-mail where that system still functions)
b) E-mail (via personal e-mail)
c) Telephone or text message to employee mobile phone number
d) News/Circulars on the Notice boards
e) Letters to all departments/units

The employees will need to be informed of the following:

a) Whether it is safe for them to come into the office
b) Where they should go if they cannot come into the office
c) Which services are still available to them
d) Work expectations of them during the disaster

Employee Contacts

Name	Role/Title	Mobile Phone Number	Personal E-mail Address

* Note: This list is available in other institutional repository

8.3Communicating with Students and Other Stakeholders

After all of the University's employees have been informed of the disaster, DICT will be responsible for informing students and other clients of the disaster and the impact that it will have on the following:

a) Anticipated impact on service offerings

b) Anticipated impact on delivery schedules
c) Anticipated impact on security of their data and information
d) Anticipated timelines

Key stakeholders will be made aware of the disaster situation first. Key stakeholders will be E-mailed first then called after to ensure that the message has been delivered. All other stakeholders will be contacted only after all key stakeholders have been contacted including research and project partner and collaborators. Each project investigator will inform his/her partners after receiving a disaster notification from the University management.

8.4Communicating with Service Providers

After all of the University's employees have been informed of the disaster, DICT will be responsible for informing service providers on the disaster and the impact that it will have on the following:

a) Adjustments to service requirements
b) Adjustments to delivery locations
c) Adjustments to contact information
d) Anticipated timelines

Key Service Providers will be made aware of the disaster situation first. They will be E-mailed first then called after to ensure that the message has been delivered. All other Service Providers will be contacted only after all Key Service Providers have been contacted.

Service Providers encompass those organizations that provide everyday services to the University, but also the suppliers of hardware and software. The Coordination Team will act as a go-between between the DR Team leads and Service Provider contacts should additional ICT infrastructure be required.

Service Provider Contacts

Company Name	Point of Contact	Phone Number	E-mail	Category

9 BACKUP AND DISASTER RECOVERY PROCEDURES

9.1Backup

The following are the steps that need to be followed to ensure back-up of data is done. In addition to data back-up automatic replication (asynchronous) need to be done for critical systems to ensure continued operations of services upon disaster occurrence.

- Server backups will be performed every business night, excluding holidays.
- Backups performed on Friday will be kept for a month before recycling.
- The last backup of every month will be considered the monthly backup and kept for a year before recycling.
- Monthly backup tapes will be stored in a fireproof safe.
- The last two monthly tapes will be stored off-site in a fireproof safe.
- Backups will be performed and monitored by a fulltime IT staff member.
- Backups will be automated using ……software or similar software product.
- Tapes will be inserted routinely every night before leaving work.
- Backup failures will be reported to the Director of Information Technology and action will be taken quickly to fix the problem.
- Backups will always be performed before upgrading or modifying a server.

9.2 Disaster Recovery

The disaster recovery process consists of five phases namely;

- Phase 1: Disaster Assessment
- Phase 2: Disaster Recovery Activation
- Phase 3: Communicating the Disaster
- Phase 4: Restoring IT Functionality

- Phase 5: Resume Normal Operations

10 DISASTER ASSESSMENT

The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Since it is almost impossible to predict when and how a disaster might occur, The University must be prepared to find out about disasters from a variety of possible avenues. These can include:

a) First hand observation
b) System Alarms and Network Monitors
c) Environmental and Security Alarms in the Primary Facility
d) Security staff
e) Facilities staff
f) End users
g) 3rd Party Vendors
h) Media reports

Once the Disaster Recovery Technical Lead has determined that a disaster had occurred, s/he must contact Disaster Management and Coordination Coordinator to officially declare that the University is in an official state of disaster. It is during this phase that the Disaster Recovery and Management Coordinator must ensure that anyone that was in the primary facility at the time of the disaster has been accounted for and evacuated to safety according to the safety Evacuation Practices depending with the nature of disaster and/or whenever necessary. *Enough Copies of DRP document should be in place and issued to relevant staff handling Disaster.*

11 DISASTER RECOVERY ACTIVATION

Once the Disaster Recovery and Management Coordinator have formally declared that a disaster has occurred s/he will initiate the activation of the DRP based on event and timings indicated in Table 10.

EVENT	DECISION
Event of fire or natural disaster affects Data Centre and Recovery sites,	Activate disaster recovery plan
Data Center destroyed (Main Server Room)	Activate disaster recovery plan
Data Center unusable for more than 2	Activate disaster recovery plan
Data Center unusable for 2 days or LESS	Disaster Recovery Technical Team perform an assessment
A System Failure for More than 2 days	Disaster Recovery Technical Team perform an assessment
Network down for more than one hour or less	Disaster Recovery Technical Team perform an assessment
Network down for more than more than hour	Disaster Recovery Technical Team perform an assessment
Environmental problems (A/C, power, etc.)	Disaster Recovery Technical Team perform an assessment

The following information will be provided to Disaster Recovery and Management Coordinator and should be passed during subsequent calls:

a) That a disaster has occurred
b) The nature of the disaster (if known)
c) The initial estimation of the magnitude of the disaster (if known)
d) The initial estimation of the impact of the disaster (if known)
e) The initial estimation of the expected duration of the disaster (if known)
f) Actions that have been taken to this point
g) Actions that are to be taken prior to the meeting of Disaster Recovery Technical Team Leads
h) Scheduled meeting place and time for the meeting of Disaster Recovery Technical Team Leads
i) Any other pertinent information

If the Disaster Recovery and Management Coordinator is unavailable for DR activation, then that responsibility shall fall to the Disaster Recovery Technical Lead.

12 Communicating the Disaster

Refer to the Section 3 "***Communicating during a Disaster***" for the steps need to be taken.

13 Restoring IT Functionality, Data and Services

Should a disaster actually occur and MUHAS need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which the University's information system will be recovered.

In general, before any employees can enter or assess the affected facility after a disaster, appropriate authorities including Fire and Rescue Force must first ensure that the premises are safe to enter.

Once safety measures are taken the Disaster Recovery technical team will assess the nature and the magnitude of the disaster by examining Networks, Servers, data, applications and other operations of any equipment of MUHAS Network. During the review of all necessary areas, they must assess any areas where further damage can be prevented and take the necessary means to protect the university's assets. Any necessary repairs or preventative measures must be taken to protect the facilities and equipment; these costs must first be approved by the Disaster Recovery Management and Coordination Team.

The system recovery process should follow the order of:

(a) Recovering baseline infrastructure first: Facilities, networks, telecom and other baseline infrastructure needed to support servers, applications and communications.
(b) Application and Client Hardware: Server, desktop, phone system
(c) Application, software, data
(d) Interfacing systems
(e) End user access and turnover

14 Restoring Server Operations

These procedures outline the steps required to restore any of MUHAS's servers. Recovery

for the servers assumes that:

- Good backup data exists and can be retrieved from offsite storage
- Replacement servers will be procured with equal or greater capacity
- All the software packages are available for installation
- Network connectivity will be re-established

A decision must be made as to where the recovery will take place (alternate site, primary location). This decision is not made ahead of time since the specifics of the incident requiring recovery is not known. The steps to restore server operations are as indicated in Table 11. It needs to be noted that some steps are not applicable to all disaster situations.

Table 11: Steps to restore server operations

STEP	TASK DESCRIPTION
Step 1	Assess the damage
Step 2	Prioritize servers to recover (DNS, Epicor, SARIS, Mail, Web etc.)
Step 3	Activate back up servers or order replacements for damaged equipment from vendors
Step 4	Order appropriate cables, wires and network devices
Step 5	Configure hardware as it arrives
Step 6	Retrieve the backup hard drive from offsite storage
Step 7	Test Server hardware
Step 8	Install appropriate operating system on the server. Refer to the server info sheets to install the correct releases
Step 9	Install network cards (If not present)
Step 10	Install cables on the server
Step 11	Restore backed up data to the available disk drives using Windows Backup (for window based operating system, and FTP or SSH for Linux based operating systems)
Step 12	Connect the servers to the network
Step 13	Start applications for user verification
Step 14	Contact users and coordinate verification
Step 15	Verify user access to network
Step 16	Resume normal processing

15 Restoration of Application, Software and Data

In case loss of data is discovered, evaluation and investigation by IT staff is immediately dispatched. In most cases, loss of data is related to file corruption, virus, security or human error. If loss of data is related to data corruption, IT Staff must troubleshoot and determine if the problem is hardware or software related to prevent addition file corruption. If the loss of data is related to a virus, IT Staff must determine the extent of the virus and remove it to prevent further loss of data. If the loss of data is related to security or a compromised system, IT Staff must determine the extent of the compromise and fix the vulnerability quickly to prevent further loss of data. If the loss of data is related to human error, IT Staff must immediately inform and train the appropriate personnel to avoid further loss of data. Once the problem has been determined and loss of data minimized, IT Staff should proceed to restoration of data from backup media. The steps to restore data are as indicated in Table 11. It needs to be noted that some steps are not applicable to all disaster situations.

Table 11: Steps to restore data

STEP	TASK DESCRIPTION
Step 1	Determine the time and date of the lost data
Step 2	Determine the appropriate backup media to restore the data
Step 3	Insert the backup media into the appropriate server.
Step 4	Invoke the Backup/Restore software
Step 5	Schedule the restore of the appropriate data within the Backup/Restore software
Step 6	Monitor the restore of data.
Step 7	Upon restore, evaluate the integrity of the restored data.
Step 8	Contact the end-user of the data to finalize restore.
Step 9	Upon approval from the end-user, the restore is considered finished.

16 Resume Normal Operations

This phase involves the reactivation of the primary data center at either the original or possibly a new location. The activation of this site does not have to be as rushed as the activation of the alternate recovery center. At the end of this phase, a thorough review of the disaster recovery

process should be taken. Any deficiencies in this plan can be corrected by updating the plan. Once the threat has passed, equipment has been repaired or replaced or a new data center has been built and stocked, operations the disaster recovery team will assess the situation, declare the disaster over and resume normal.

17 THE DISASTER RECOVERY TEAMS AND RESPONSIBILITIES

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of the University. The different groups and their responsibilities are as follows:

(a) Disaster Recovery Management and Coordination Team

(b) Disaster Technical Team

17.1 Disaster Recovery Management and Coordination Team

The disaster recovery coordination team shall be headed by the Disaster Recovery Coordinator. The function of the Disaster Recovery Coordinator is to maintain the plan in a consistent state of readiness. The primary responsibility of the Disaster Recovery Management and Coordination team is to:

(a) Distribution of the Disaster Recovery Plan
(b) Ensure Disaster Recovery Teams are trained
(c) Ensure the Disaster Recovery Plan is tested
(d) Ensure Disaster Recovery Plan Tests are conducted
(e) Ensure, in the event of Disaster, all necessary communications are held to stakeholders.
(f) Assess the damage and if necessary, declare a disaster (damage assessment Forms are included in this plan)
(g) Secure financial backing for the recovery effort
(h) Approve all actions that were not pre-planned
(i) Give strategic direction
(j) Be the liaison to upper/University management
(k) Expedite matters through all bureaucracy

In a disaster situation, the Disaster Recovery Coordinator will:

(a) Make the determination that a disaster has occurred and trigger the DRP and related processes.

(b) Initiate the DR Call Tree.
(c) Be the single point of contact for and oversee all of the DR Teams.
(d) Organize and chair regular meetings of the DR Team leads throughout the disaster.
(e) Present to the DICT Management Team on the state of the disaster and the decisions that need to be made.
(f) Organize, supervise and manage all DRP tests and author all DRP updates.
(g) Facilitate communication between technical and non-technical staff
(h) Act as a Project Manager to coordinate the efforts of

- Technical staff
- Academic and administrative staff
- Vendors
- University Management
- Other personnel as needed

The ICT Disaster Recovery Coordinator at MUHAS is the Director of ICT, assisted by one technical ICT staff.

CONTACTS

NAME	TELEPHONE	FUNCTIONAL ASSIGNMENT
Dr. Felix Sukums	0713238473	Coordination and reporting to the University Management
Mr. Hassan Sengo	0713338452	
Mr. Pius Maswaga	0713993982	

Note: The Team will be headed by Coordinator whose contact details are provided in Table above.

17.2 DISASTER RECOVERY TECHNICAL TEAM

The Technical Network Team will be responsible for assessing damage specific to any physical infrastructure required for the University to run its IT operations and applications in the event of and during a disaster. The team will oversee technical issues in the event of disaster that include but not limited to Servers, Networks, Applications, Software and Data. They will be primarily responsible for providing baseline technical services to ensure the recovery of services. Other Tasks includes of the team includes.

(a) Make recommendations on how the disaster recovery plan can be improved.
(b) Set the DRP into motion after the Disaster Recovery Coordinator has declared a disaster
(c) Determine the magnitude and class of the disaster
(d) Determine what systems and processes have been affected by the disaster

(e) Keep a record all activities done during the disaster recovery process

(f) Ensure that all decisions made abide by the DRP and policies set by the University

(g) Install and implement any tools, hardware, software and systems required to solve the problem.

(h) Get the secondary site ready to restore business operations

(i) Ensure that the primary and secondary site (if available) is fully functional and secure

(j) Create a detailed report of all the steps undertaken in the disaster recovery process

(k) Notify the relevant parties once the disaster is over and normal business functionality has been restored

(l) After the University is back to business as usual, this team will be required to summarize all activities done and will provide a report to the Disaster Recovery Coordinator summarizing their activities during the disaster and associated cost (if any)

CONTACTS

NAME	TELEPHONE	FUNCTIONAL ASSIGNMENT
Mr. Hassan Sengo		*System Administrator*
Mr. Pius Maswaga		*System Administrator*
Mr. Asanali Msangi		*System Administrator*
Mr. Juma Singano		*System Administrator*

17.3 TRAINING THE DISASTER RECOVERY TEAM

The Disaster Recovery and Management Coordinator is responsible for the coordination of training relating to the disaster recovery plan. It is the responsibility of each member of recovery team's participant to fully read and comprehend the entire plan, with specific emphasis on their role and responsibilities as part of the recovery team.

18 TESTING AND MAINTAINING THE DISASTER RECOVERY PLAN

While efforts will be made initially to construct this DRP is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

18.1 Maintenance and Review

The DRP will be updated annually or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery and Management Coordinator will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the university in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

a) Ensuring that call trees are up to date
b) Ensuring that all team lists are up to date
c) Reviewing the plan to ensure that all of the instructions are still relevant to the organization
d) Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals
e) Ensuring that the plan meets any requirements specified in new laws and regulations
f) Other organizational specific maintenance goals

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the University, it is the responsibility of the Disaster Recovery and Management Coordinator to appoint a new team member.

18.2 Testing

The Disaster Recovery and Management Coordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. On an on-going basis this frequency appears to be adequate considering the systems involved. However, special tests are to be given consideration whenever there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of testing the disaster recovery plan are as follows:

- Simulate the conditions of an ACTUAL Business Recovery situation.
- Determine the feasibility of the recovery process
- Identify deficiencies in the existing procedures
- Test the completeness of the business recovery information stored at the Offsite Storage Location.
- Train members of the disaster recovery teams

Testing the plan will be carried out as follows:

a) **Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).

b) **Simulations-** A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyse the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of

the cycle have been applied.

c) **Parallel Testing-** A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.

d) **Full-Interruption Testing-** A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.

Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery and Management Coordinator as well as any resources that he/she will require. The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Disaster Recovery and Management Coordinator that are cost effective and meet the benefits and objectives desired.

APPENDIX 1: MUHAS ICT NETWORK DIAGRAM

APPENDIX 2: LIST OF ICT SERVICES

APPENDIX 3: LIST OF ICTSYSTEMS

ICT Infrastructure and Services	Location
Data Centre/Server Room at MUHAS	MPL 4TH FLOOR /CHIPE 1ST FLOOR
Data Centre/Server Room at MAMC	3rd FLOOR
Network Services (LAN) for staff	MUHAS CAMPUS ALL BLOCKS
Network Services (LAN) for MAMC	3rd FLOOR
Network Names System (DNS) for MUHAS	MPL SERVER ROOM
Health Management Information System (HMIS) for MAMC	3rd FLOOR
Picture Archival and Communication System (PACS)	3rd FLOOR
Dental Clinic Information System (include financial module)	DENTAL
Internet Connectivity for Mloganzila Campus	3rd FLOOR
Internet Connectivity for MUHAS Campus	MPL 4TH FLOOR
Financial Information System (Epicor 9) for MUHAS	MPL 4TH FLOOR
Financial Information System (Epicor 10) for MAMC	3rd FLOOR
Student Academic Information System (SARIS)	MPL 4TH FLOOR
Email Service for Staff	MPL 4TH FLOOR
ESET Endpoint Security	MPL 4TH FLOOR
VOIP service at MUHAS	MUHAS BLOCKS
VOIP service at MAMC	GROUNG FLOOR
Whole of MUHAS network infrastructure (all campuses)	

APPENDIX 4: MUHAS Network Switches details (MAIN CAMPUS)

Make/Model	Description	IP	Misc. Details
Catalyst 3750 Series	Located at DICT	192.168.0.31	Back Bone Switch
Catalyst 2960 Series	Located at Server Room 48 Ports Switch	192.168.0.220	New Switch at Server Room 48 Ports
Catalyst 2950 Series	Located at Router Room 24 Ports	192.168.0.239	Router Room Switch
Catalyst 3550 Series	Located at MNH	192.168.25.5	MUHAS Switch at MNH
Catalyst 2950	Located at ITM	192.168.11.2	ITM 1
Catalyst 2950	Located at Library	192.168.14.2	Lib 1
Catalyst 2950	Located at Pharmacy	192.168.13.2	Pharm 1
Catalyst 2950	Located at PRO Admin	192.168.15.2	PRO Office Switch
Catalyst 2950	Server room 24 Port Switch	192.168.0.12	Server room Old Switch
Catalyst 2950	Located at CHB	192.168.12.2	CHB 1
Catalyst 2950	Located at Undergraduate	192.168.17.2	Optic Fiber Switch

Catalyst 2950	Located at Accounts 1st Floor	192.168.19.2	Accounts Floor1
Catalyst 2960	Library Server Room	192.168.22.2	Library Server
Catalyst 2950	Located at MPH	192.168.10.2	MPH 1
Catalyst 2950	Located at IAHS	192.168.24.12	IAHS Fiber Switch
Catalyst 2950	Located at Dental	192.168.25.3	Dental Fiber Switch
Catalyst 2950	Located at Undergraduate Lab	192.168.17.4	
Catalyst 2950	Located at CHB	192.168.13.3	CHB2
Catalyst 2950	Located at New Office Block Server Room	192.168.16.2	Server Room New Office Block
Catalyst 2950	Located at ITM	192.168.11.3	ITM 2
Catalyst 2950	Located at Undergraduate	192.168.17.9	Undergraduate 5
Catalyst 2950	Located at Undergraduate	192.168.17.4	Undergraduate 3
Catalyst 2950	Located at Undergraduate	192.168.17.3	Undergraduate 2
Catalyst 2950	Located at MPH	192.168.10.3	MPH 2
Catalyst 2950	Located at Procurement Office	192.168.19.4	Procurement office On Accounts Ground Floor
Catalyst 2950	Located at DICT	192.168.17.6	DICT 1
Catalyst 2950	Located at Library Server	192.168.22.3	Library Server switch2
Catalyst 2950	Located at Dental Building	192.168.25.2	Dental Switch 1
Catalyst 2950	Located at Dental Restorative	192.168.25.9	Restore Dental Switch
Catalyst 2950	Located at Dental	192.168.25.4	Switch 3
Catalyst 2950	MDH Switch	192.168.19.13	MDH Switch
Catalyst 2950	Located at DICT	192.168.17.5	DICT 2
Catalyst 2950	Located at MPL 3rd Floor	192.168.16.3	MPL 3rd Floor
Catalyst 2950	Located at New Office Block	192.168.16.5	New Office Block First Floor
Catalyst 2960	Located at Library Server Room	192.168.22.4	Library Server Switch 3
Catalyst 2950	Located at New Office Block	192.168.16.4	Third Floor Switch 3
Catalyst 2950	Located at New Office Block	192.168.16.8	Ground Floor Switch
Catalyst 2950	Located at undergraduate Lab	192.168.17.7	Undergraduate 6
Catalyst 2950	Located Server Room	192.168.0.10	Rack Switch
Catalyst 2960 Series	Located at Dental 1st	192.168.27.5	Dental Switch 1st Floor

	Floor		
Catalyst 2960 Series	Located at ESTATE	192.168.14.3	Estate Switch1
Catalyst 2960 Series	Located at CHIPE Server Room	192.168.21.2	CHIPE Server Room Switch
Catalyst 2960 Series	Located at Internal Medicine	192.168.14.4	Internal Medicine Switch 1
Catalyst 2960 Series	Located at Nursing Skilled Lab		Nursing Skilled Lab Switch
Catalyst 2960 Series	Located at MPH	192.168.10.50	MPH Switch 3
Catalyst 2960 Series	Located at Library Server Room	192.168.22.5	Library Server Switch 5
Catalyst 3750 Series	Located at DICT	192.168.0.31	Back Bone Switch
Catalyst 2960 Series	Located at Server Room 48 Ports Switch	192.168.0.220	New Switch at Server Room 48 Ports
Catalyst 2950 Series	Located at Router Room 24 Ports	192.168.0.239	Router Room Switch
Catalyst 3550 Series	Located at MNH	192.168.25.5	MUHAS Switch at MNH
Catalyst 2950	Located at ITM	192.168.11.2	ITM 1
Catalyst 2950	Located at Library	192.168.14.2	Lib 1
Catalyst 2950	Located at Pharmacy	192.168.13.2	Pharm 1
Catalyst 2950	Located at PRO Admin	192.168.15.2	PRO Office Switch
Catalyst 2950	Server room 24 Port Switch	192.168.0.12	Server room Old Switch
Catalyst 2950	Located at CHB	192.168.12.2	CHB 1
Catalyst 2950	Located at Undergraduate	192.168.17.2	Optic Fiber Switch
Catalyst 2950	Located at Accounts 1st Floor	192.168.19.2	Accounts Floor1
Catalyst 2960	Library Server Room	192.168.22.2	Library Server
Catalyst 2950	Located at MPH	192.168.10.2	MPH 1
Catalyst 2950	Located at IAHS	192.168.24.12	IAHS Fiber Switch
Catalyst 2950	Located at Dental	192.168.25.3	Dental Fiber Switch
Catalyst 2950	Located at Undergraduate Lab	192.168.17.4	

APPENDIX 5: MAMC Network switch details.

NanoStation M5	NANOSTATIOON CHIPE-MPL GW	192.168.0.162	CHIPE-MPL GW
NanoStation M5	CPL-MPL NANO STATION	192.168.0.98	CPL-MNH
NanoStation M5		192.168.0.6	HIVIS-MUHAS
NanoStation M5	NANOSTATION AT NIMR	192.168.0.7	NIMR-NANO
NanoStation M5	NANOSTATION AT TAKASHIN	192.168.0.64	TAKASHIN-CPE
NanoStation M5	CHIPE-MAIN-RT	192.168.0.163	CHIPE-MAIN-RT
NanoStation M5	NANOSTATION AT MPL	192.168.0.189	MPL-GW6
NanoStation M5	NANOSTATION AT TDA	192.168.0.50	TDA-AP
NanoStation M5	NANOSTATION AT MUHAS	192.168.0.94	MUHAS-AP
Mikrotik RouterOS	Mikrotik AP	10.0.0.50	MUHAS AP L45-01
Mikrotik RouterOS	Mikrotik AP	10.0.0.16	MUHAS PHYS-01
Mikrotik RouterOS	Mikrotik AP	10.0.0.21	MUHAS LIB-01
Mikrotik RouterOS	Located at Block M	10.0.0.19	MUHAS AP BLOCK-M
Mikrotik	MUHAS AP Located at Physiology	10.0.0.17	MUHAS AP Physiology 2
Mikrotik	MUHAS AP CHB	10.0.0.18	CHB AP
Mikrotik	MUHAS AP PHARMACY	10.0.0.18	AP PHARM 01
Mikrotik	MUHAS AP Located at Library first floor	10.0.0.22	AP Library 11

APPENDIX 6: MAMC Network Access Point details.

MUHAS Network Switches details (MAMC)			
BlackDiamond 8810	Main Backbone switch located in Server room	192.168.30.1	MGT
Exteme Summit x430-24t	Work Group Switch	192.168.30.11	Basement zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.12	Basement zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.13	Basement zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.14	Ground floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.15	Ground floor zone A

Exteme Summit x430-24t	Work Group Switch	192.168.30.16	Ground floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.17	Ground floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.18	Ground floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.19	Ground floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.20	Ground floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.21	Ground floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.22	Ground floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.23	Ground floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.24	Ground floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.25	First floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.26	First floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.27	First floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.28	First floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.29	First floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.30	First floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.31	First floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.32	First floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.33	First floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.34	First floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.35	First floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.36	First floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.37	Second floor zone A
Exteme Summit x430-	Work Group Switch	192.168.30.38	Second floor zone A

24t			
Exteme Summit x430-24t	Work Group Switch	192.168.30.39	Second floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.40	Second floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.41	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.42	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.43	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.44	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.45	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.46	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.47	Second floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.48	Third floor
Exteme Summit x430-24t	Work Group Switch	192.168.30.49	Third floor
Exteme Summit x430-24t	Work Group Switch	192.168.30.50	Third floor
Exteme Summit x430-24t	Work Group Switch	192.168.30.51	Third floor
Exteme Summit x430-24t	Work Group Switch	192.168.30.52	Third floor
Exteme Summit x430-24t	Work Group Switch	192.168.30.53	Third floor
Exteme Summit x430-24t	Work Group Switch	192.168.30.54	Fourth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.55	Fourth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.56	Fourth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.57	Fourth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.58	Fourth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.59	Fourth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.60	Fifth floor zone A

Exteme Summit x430-24t	Work Group Switch	192.168.30.61	Fifth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.62	Fifth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.63	Fifth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.64	Fifth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.65	Fifth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.66	Fifth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.67	Sixth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.68	Sixth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.69	Sixth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.70	Sixth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.71	Sixth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.72	Sixth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.73	Sixth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.74	Seventh floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.75	Seventh floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.76	Seventh floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.77	Seventh floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.78	Seventh floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.79	Seventh floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.80	Seventh floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.81	Eighth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.82	Eighth floor zone A
Exteme Summit x430-	Work Group Switch	192.168.30.83	Eighth floor zone A

24t			
Exteme Summit x430-24t	Work Group Switch	192.168.30.84	Eighth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.85	Eighth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.86	Eighth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.87	Ground floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.88	Ninth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.89	Ninth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.90	Ninth floor zone A
Exteme Summit x430-24t	Work Group Switch	192.168.30.91	Ninth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.92	Ninth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.93	Ninth floor zone B
Exteme Summit x430-24t	Work Group Switch	192.168.30.94	Mortuary

APPENDIX 7: MAMC NETWORK ACCESS POINT DETAILS.

Aerohive AH-AP-230	Wireless Access Points	192.168.30.101	Ground floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.102	Ground floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.103	Ground floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.104	Ground floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.105	First floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.106	First floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.107	First floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.108	First floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.109	First floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.110	Second floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.111	Second floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.112	Second floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.113	Second floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.114	Third floor
Aerohive AH-AP-230	Wireless Access Points	192.168.30.115	Third floor
Aerohive AH-AP-230	Wireless Access Points	192.168.30.116	Third floor
Aerohive AH-AP-230	Wireless Access Points	192.168.30.117	Fourth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.118	Fourth floor zone B

Aerohive AH-AP-230	Wireless Access Points	192.168.30.119	Fifth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.120	Fifth floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.121	Sixth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.122	Sixth floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.123	Seventh floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.124	Seventh floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.125	Eighth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.126	Eighth floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.127	Ninth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.128	Ninth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.129	Ninth floor zone A
Aerohive AH-AP-230	Wireless Access Points	192.168.30.130	Ninth floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.131	Ninth floor zone B
Aerohive AH-AP-230	Wireless Access Points	192.168.30.132	Ninth floor zone B