University of Fort Hare

Together in Excellence

ICT Disaster Preparedness and Recovery Plan

Version 1.5

March, 2016

Proposed University of Fort Hare ICT Disaster Preparedness and Recovery Plan

Version 1.4 – May 2015

Acknowledgments

This document has been prepared by C.P. Johl from a template jointly created by the ICT Directors of the Eastern Cape Region and will be reviewed by the Information Technology Division and approved by the Executive Management Team.

1.0 Purpose and Scope

===

1.1 Introduction

UFH has a highly computerized operational environment. This includes the use of personal computers in offices as well as several Microsoft, Unix and Linux servers that provide much of the operational support for the administrative and academic units. A wide area network ties these various systems together and provides communications to other computer networks and universities. In addition, the operation of the Delivery Site network provides a vital support component of the University system, including the operation of local and long distance telephone services.

The reliability of computers and computer-based systems has increased dramatically over the past years, and the computer failures that do occur can normally be diagnosed automatically and repaired promptly using both local and remote diagnostic facilities. Many computer systems contain redundant parts, which improve their reliability and provide continuity of operation when some failures occur.

In the past, many administrative computer operations were predominantly off line and disaster plans were comprised of reciprocal agreements between users of similar systems for batch job processing (usually at night or over week-ends).
This has become less feasible with the very complicated on-line and diverse network systems most institutions now have in place. Although institutions may have similar equipment and operating systems, they generally do not have the capacity to add large numbers of users from another on-line environment to their systems even if other technical and software licensing problems could be solved.

A trend is evolving to provide alternate sites near the central systems where any additional equipment needed can be shipped in rapidly, and where critical on-line operations for the organization can be resumed within a reasonable time. Redundancy in the communications network and a tie-in to the alternate site, or the ability to rapidly tie-in, is an important part of a disaster plan. This type of site is called a cold backup site, as opposed to a hot backup site which contains all equipment necessary to start immediate operations.

For the most part, the major problems that can cause a computing system to be inoperable for a length of time result from environmental problems related to the computing systems. The various situations or incidents that can disable, partially or completely, or impair support of UFH's computing facilities are identified. A working plan for how to deal with each situation is provided.

Almost any disaster will require special funding from the University in order to allow the affected systems to be repaired or replaced. This report assumes that these funds will be made available as needed. Proper approval will be obtained before any funds are committed for recovery. A specific emergency funding process will be designed and implemented for this purpose.

1.2 Objectives/Constraints

A major objective of this document is to define procedures for a contingency plan for recovery from disruption of computer and/or network services. This disruption may come from total destruction of the central site or from minor disruptive incidents. There is a similarity in the procedures required to deal with the different types of incidents affecting different departments in UFH's Information

Technology areas. However, special attention and emphasis is given to an orderly recovery and resumption of those operations that concern the critical business of running the University, including providing support to academic departments relying on computing. Consideration is given to recovery within a reasonable time and within cost constraints.

The objectives of this plan are limited to the computing support given to UFH clients from the Information Technology Division, including academic and administrative systems under the stewardship of the Information Technology Division.
The elements that concern personal computers are addressed; however, client-related functions not directly tied to computer and telephone support by the Information Technology Division are not addressed. Departments and divisions at UFH should develop their own plans to deal with manual operations within their division should computer and/or network services be disrupted (Business Continuity Planning, BCP). Hot sites will be considered as alternatives where cost factors and feasibility make this a viable alternative.

All critical computing systems that are vital for the daily operation of the University under the stewardship of the Information Technology Division must be maintained under service contracts with the equipment vendors. This ensures that routine maintenance problems will be addressed in a timely way with adequate resources. These contracts range from telephone support only to full hardware replacement.

1.3 Assumptions

This section contains some general assumptions, but does not include all special situations that can occur. Any special decisions for situations not covered in this plan needed at the time of an incident will be made by senior Information Technology Division staff members on site.

This plan will be invoked upon the occurrence of an incident. The senior staff member on site at the time of the incident or the first one on site following an incident will contact the CIO, Director of Information Technology and/or the other ICT Managers for a determination of the need to declare an incident. The Chief Operating Officer/Deputy Vice Chancellor: Institutional Support will also be notified.

The senior Information Technology staff member on site at the time of the incident will assume immediate responsibility. The first responsibility will be to see that people are evacuated as needed. If injuries have resulted or may have occurred as a result of the incident, immediate attention will be given to ensuring that those persons injured receive appropriate attention. The UFH Facilities Division will be notified if necessary. If circumstances permit, attention will be focused on shutting down systems, turning off power, etc., but evacuation is the highest priority.

Once an incident which is covered by this plan has been declared, the plan, duties, and responsibilities will remain in effect until the incident is resolved and proper University authorities are notified.

Invoking this plan implies that a recovery operation has begun and will continue with top priority until workable computer and/or telephone support to the University has been re-established.

1.3.1 Academic Computing

Academic computing is defined as the services provided to students and academic departments - namely Microsoft file service, email service, web service and public or teaching facilities/systems.

Affected systems are:

File servers at each Delivery Site, email, imap, pop, DNS, cache, web, Blackboard and ITS.

1.3.2 Administrative Computing

Administrative computing consists of the services being run on ITS, this includes services such as payroll, HR and Finance as well as the other common services listed above with the exception of Blackboard.

1.3.3 Network Communications

This consists of:

1. Local area networking - both UTP and Fiber Optic cabling on Delivery Site as well as the hubs, switches and routers used to link them.
2. Wide area networking - the Internet links and the connections to the other Delivery Sites.
3. Telephone services - both the privately maintained areas and the areas serviced by Telkom.
4. Video Conferencing services.
5. Computer Laboratories.

1.4 Incidents Requiring Action

This disaster recovery plan for UFH will be invoked under one of the following circumstances:

1. An incident which has disabled or will disable, partially or completely, the Delivery Site computing facilities, and/or the communications network for a period in excess of 24 hours.
2. An incident which has impaired the use of computers and networks managed by the Information Technology Division due to circumstances which fall beyond the normal processing of day-to-day operations. This includes all academic and administrative systems which the Information Technology Division manages.
3. An incident which was caused by problems with computers and/or networks managed by the Information Technology Division and has resulted in the injury of one or more persons at UFH.

1.5 Contingencies

General situations that can destroy or interrupt computer and communication services usually occur under the following major categories:

1. Power, including load-shedding/Air Conditioning Interruption
2. Fire
3. Water
4. Weather and Natural Phenomenon

5. Sabotage and Interdiction

There are different levels of severity of these contingencies necessitating different strategies and different types and levels of recovery. This plan covers strategies for:

1. Partial recovery - operating at an alternate site on the same or other Delivery Site and/or other client areas on Delivery Site.

2. Full recovery - operating at the current central site and client areas, possibly with a degraded level of service for a period of time.

1.6 Physical Safeguards

1.6.1 50 Church Street/Gasson Centre

The Church Street/Gasson Centre Buildings house Information Technology personnel, amongst other, as well as many of the central servers used for administrative and academic computing purposes. The computer room also contains the core of the Universitys' local area network for the area, and is the main access point for wide area network links, including those used for Internet access. The building also houses academic computing facilities in the form of laboratories and the Blackboard server.

The IT Services section is not protected at the entrance. Any UFH employees have access to this area. The file servers installed at 50 Church Street and Gasson Centre are locked behind standard doors with normal 2 or 3 level locks.

These East London sites are not covered by an electronic fire protection system but CO2 or fire extinguishers are available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

Critical File Servers and main routing equipment in the File Server room are powered by a single 30 KVA 3 Phase UPS unit. There is a Diesel generator backup on this site.

This room also houses a telephone PABX, and other data communications equipment. It is a hub for the University networks.

The telephone equipment is connected to the UPS system.

1.6.2 Bhisho Delivery Site Building

The PFSA Bhisho Delivery Site Building houses Information Technology personnel, amongst other as well as many servers used for administrative and academic computing purposes. The computer room also contains the core of the University's local area network for the building.

This Administration block houses a telephone PABX, and other data communications equipment. The telephone equipment is connected to the UPS system. There is a standby generator at this site.

The IT Services section has no electronic access control protection once inside the PFSA building, with the exception of keys.

The PFSA Bhisho Delivery Site Building is covered by a fire detection system. CO2 or fire extinguishers are available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

The PFSA Bhisho Delivery Site Building is powered by an 8 KVA 3 Phase UPS that is capable of holding the load for 30 minutes to shut the services down cleanly and has a 12 KVA 3 Phase UPS Standby Generator installed.

1.6.3 Alice Delivery Site

The main ICT offices on Alice campus are on the ground floor of the Chemistry block. The unit is comprised of a closed and access controlled computer room, a technical repair and maintenance area and other lockable offices.

Entry to the ICT area is not controlled.

A Halon gas full auto/manual fire suppression system is installed, and the room is cooled by air conditioning units. The unit is regularly serviced by the maintenance team.

The Siemens telephone PABX, and other data communications equipment is housed in Administration block.

The Alice Campus computer area is served with a standby generator plant. This has failed and is in the process of being replaced.

In addition, a 50 KVA 3 Phase UPS gives the computer room some forty minutes of standby power in the event that the backup generator does not power up.

The telephone equipment is connected to a small UPS system and standby plant which will maintain the telephone switch for as long as the standby plant is fuelled.

There is no protection against water damage other than a raised floor in the computer room.

No monitoring system has been installed.

1.6.4 Nursing Sciences delivery site building

The Nursing Sciences delivery site houses no Information Technology personnel.

There are no servers at the Nursing Sciences site and all network services are derived from main servers at the East London campus. Entry to the site is guarded with 24x7 guards.

Nursing Sciences delivery site buildings are not covered by a fire detection system and there are CO2 fire extinguishers available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

Nursing Sciences delivery site has no UPS and power failure will result in the loss of all communications.

1.6.5 Accounting delivery site building

The Accounting delivery site houses no Information Technology personnel.

There are no servers at the Accounting site and all network services are derived from main servers at the East London campus. Entry to the site is guarded with 24x7 guards.

Accounting delivery site buildings are not covered by a fire detection system and there are CO2 fire extinguishers available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

Accounting delivery site has no UPS and power failure will result in the loss of all communications.

1.6.6 GMRDC delivery site building

The GMRDC delivery site houses no Information Technology personnel.

There are no servers at the GMRDC site and all network services are derived from main servers at the East London campus. Entry to the site is guarded with 24x7 guards.

GMRDC delivery site buildings are not covered by a fire detection system and there are CO2 fire extinguishers available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

GMRDC delivery site has no UPS and power failure will result in the loss of all communications.

1.6.7 Miriam Makeba delivery site building

The Miriam Makeba delivery site houses no Information Technology personnel.

There are no servers at the Miriam Makeba site and all network services are derived from main servers at the East London campus. Entry to the site is guarded with 24x7 guards.

Miriam Makeba delivery site buildings are not covered by a fire detection system and there are CO2 fire extinguishers available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

Miriam Makeba delivery site has no UPS and power failure will result in the loss of all communications.

1.6.8 Planning and J&J Institute delivery site building

The Planning and J&J Institute delivery site houses no Information Technology personnel.

There are no servers at the Planning and J&J Institute site and all network services are derived from main servers at the East London campus. Entry to the site is guarded with 24x7 guards.

Planning and J&J Institute delivery site buildings are not covered by a fire detection system and there are CO2 fire extinguishers available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

Planning and J&J Institute delivery site has no UPS and power failure will result in the loss of all communications.

1.6.9 Education delivery site building

The Education delivery site houses no Information Technology personnel.

There are no servers at the Education site and all network services are derived from main servers at the East London campus. Entry to the site is guarded with 24x7 guards.

Education delivery site buildings are not covered by a fire detection system and there are CO2 fire extinguishers available at strategic points in the building.

There is no protection against water damage.

There is no monitoring system installed.

Education delivery site has no UPS and power failure will result in the loss of all communications.

1.7 Types of Computer Service Disruptions

This document includes hardware and software information, emergency information, and personnel information that will assist in faster recovery from most types and levels of disruptive incidents that may involve UFH's computing facilities. Additional information that may be needed is provided in the appendices of this document. Supporting documents contain additional hardware, software and vendor information.

1.7.1 Normal computer system problems

For most of the major hardware vendors represented on Delivery Site, as well as some of the software vendors, remote diagnostic testing is available for routine problems.
Normal response is within four hours for hardware problems.
UFH has maintenance contracts for these systems.

Hardware parts for the Unix servers are available through Dimension Data who has back-to-back service agreements with Hewlett Packard.

Some minor hardware problems do not disrupt service and maintenance is scheduled when convenient for these problems.

1.7.2 Major computer and communications system problems

Experiences at UFH with Dimension Data in solving more severe computer problems have shown that they have backup strategies.
If the local service personnel have not fixed the problem within a few hours, they can call for backup support from Port Elizabeth or other locations as needed. Further, if parts are not available locally or in these close backup areas, parts have been flown in and received within 24 hours.

The only local stock kept is peripheral devices that can be replaced without affecting the equipment warranty.

1.7.3 Environmental problems (air conditioning, electrical, fire)

1.7.3.1 Air Conditioning Outage

The maintenance department within UFH is responsible for the running of air-conditioning units.

1.7.3.2 Electrical

In the event of an electrical outage some servers and other critical equipment are protected from damage by Uninterruptible Power Supplies (UPS's). These units will maintain electrical service to our servers long enough for them to be shut down gracefully. Once electrical power is restored the servers will remain "powered down" until the UPS's are recharged sufficiently to ensure the servers could be gracefully shut down in the event of a second power failure.

1.7.3.3 Fire

Only the computer centre at Alice Delivery Site has an automated Halon gas system installed.

In the event of a catastrophic fire involving the entire building, it would most likely be necessary to replace all our hardware. UFH critical data is backed up daily and stored in the safes adjacent to the computer room at Alice campus and the safe adjacent to room 124, 1st floor Gasson Center in East London.

1.8 Insurance Considerations

Key Unix servers and networking infrastructure components are covered by hardware maintenance contracts. Additionally, all major hardware is covered under UFH's standard property and casualty insurance for the University.

2.0 Recovery Team

In case of a disaster, the team will use the emergency call list. General duties of the disaster recovery coordinator are discussed. Recovery team leaders have been assigned in each major area and general duties given. Assignment of personnel in the major areas to specific tasks during the recovery stage will be made by the team leader over that area.

It is recognized that the Information Technology Division may not have the resources required to undertake recovery operations in the event of a major disaster. However other Departments in the University have suitably qualified personnel that may be able to assist in such operations.
If feasible, and if appropriate, such personnel should be made available in the event of major disasters. Before such personnel are deployed, clearance will be obtained from their Head of Department or Manager.

2.1 Organization of the Disaster/Recovery Team

2.1.1 Disaster Recovery Coordinator

Chief Information Officer (CIO)

2.1.2 Delivery Site Recovery Team

Supervisor, ICT
Software analyst
IT Support Officer

2.1.3 Network Communications Recovery Team

Communications Supervisor
Network Administrator
Telecom Analysts

2.2 Disaster/Recovery Team Headquarters

- The senior officials' office of Delivery Site ICT Services will be used as the meeting venue if the building is safe.
- If the Delivery Site ICT Services office is not usable then any other designated office may be used as indicated by the CIO.
- If none of the Delivery Site facilities are usable, it is presumed that the disaster is of such proportions that recovery of computer support will take a lesser priority. The Disaster Recovery coordinator will make appropriate arrangements.

2.3 Disaster Recovery Coordinator

The CIO will serve as Disaster Recovery Coordinator. The major responsibilities include:

- Determining the extent and seriousness of the disaster, notifying the Chief Operations Officer (COO) immediately and keeping him informed of the activities and recovery progress. The COO will in turn keep the Vice Chancellor and other senior University management informed.
- Invoking the Disaster Recovery Plan.
- Supervising the recovery activities.
- Coordinating with the Chief Operating Officer on priorities for clients while going from partial to full recovery.

- Obtaining clearance from Departments or Divisions who have suitably qualified personnel that may be of assistance in carrying out recovery procedures.

- Naming replacements, when needed, to fill in for any disabled or absent disaster recovery members. Any members who are out of town and are needed will be notified to return.

- The ICT Supervisor will keep clients informed of the recovery activities.

2.5 Network Communications Recovery Team Leader Responsibilities

The ICT Supervisor in whose area of responsibility the disaster occurs will serve as the Network Communications Recovery Leader.

Responsibilities include:

- Coordinating hardware and software replacement with the communications hardware and software vendors.

- Supervising recovery of the computer communications and telephone system.

- Assigning personnel duties from telecom analysts to project leaders of disaster recovery tasks as needed.

- Coordinating activities of computer and communications recovery with the other Recovery Team Leaders.

- Keeping the Disaster Recovery Coordinator informed of the extent of damage and recovery procedures being implemented.

3.0 Preparing for a Disaster

This section contains the minimum steps necessary to prepare for a possible disaster and as preparation for implementing the recovery procedures. An important part of these procedures is ensuring that the off-site storage facility contains adequate and timely computer backup tapes and documentation for applications systems, operating systems, support packages, and operating procedures.

3.1 General Procedures

Responsibilities have been given for ensuring each of following actions have been taken and that any updating needed is continued.

- Maintaining and updating the disaster recovery plan.

- Ensuring that all Information Technology Division personnel are aware of their responsibilities in case of a disaster.

- Ensuring that periodic scheduled rotation of backup media is being followed for the off-site storage facilities.

- Maintaining and periodically updating disaster recovery materials, specifically documentation and systems information, stored in the off-site areas.
- Maintaining a current status of equipment in the main equipment rooms.
- Informing all Information Technology Division personnel of the appropriate emergency and evacuation procedures from the buildings.
- Ensuring that all security warning systems and emergency lighting systems are functioning properly and are periodically checked by operations personnel.
- Ensuring that fire protection systems are functioning properly and that they are checked periodically, where applicable.
- Ensuring that UPS systems are functioning properly and that they are being checked periodically.
- Ensuring that the client community is aware of appropriate disaster recovery procedures and any potential problems and consequences that could affect their operations.
- Ensuring that the operations procedure manual is kept current.
- Ensuring that proper temperatures are maintained in equipment areas.

3.2 Software Safeguards

Administrative software and data are secured by full backups each week and differential backups each weekday evening. The full backups are transported each Monday morning to the ICT Services safe on Delivery Site. The last backup of each month is retained for one year. Nightly differential backups are retained in ICT Services safe on Delivery Site. A copy of the full backups is also stored in the safe adjacent to room 122 Gasson Centre.
Backups are stored on magnetic tapes and other compact media.

Academic Computing software and data are secured by full backups each week and differential backups each evening. On nights when a full backup is not done on a disk, differential backups are done on that disk. The full backups are transported each Monday morning to the ICT Services safe on Delivery Site. A copy of the full backups is also stored in the safe adjacent to room 124 Gasson Centre.
The last full backup of each month is retained for one year. Nightly differential backups are retained until the next full backup. Backups are stored on 4mm DAT tapes and other compact media.

Telephone call data is backed up daily and also immediately before each monthly billing cycle. These monthly backups are kept for the year.
Disposal dates for the saved sets are not currently implemented. Call records are routed through a call buffer. This captures call records while the logging computer is unavailable. The buffer will capture approximately a thousand calls, which is around two and one-half to three days of calls during the busy time of the month.

Telephone switch software and data are secured by a full backup each night to CD-RW. The diskette left in the telephone switch is overwritten each night. Each Monday morning, the CD-RW is removed and transported to the ICT Services safe on Delivery Site. There are CD-RW in rotation for the full backups.

4.0 Recovery Procedures

4.1 Server Facilities Recovery Plan

An incident at the computing/networking facilities in any of the UFH Delivery Sites may place this plan into action. An incident may be of the magnitude that the facilities are not usable and alternate site plans are required. In this case, the alternate site portions of this plan must be implemented. It is obvious that all major support sections in Information Technology Division areas will need to function together in a disaster, although a specific plan of action is written for each section.

Two Hewlett Packard DL585 G5 file servers situated at the Main Campus Building and the Gasson Centre Buildings on East London delivery site running ITS Version Integrator 1.0 for the entire UFH. The servers are virtualized and run both the application and database server instances. **There are two other servers in Gasson Centre to host the ITS Disaster Recovery system that will operate automatically should the main servers fail.** The servers running the ITS software are defined as a critical systems. Hardware support is provided by Dimension Data East London on a time and material basis. There is a Service Level Agreement on the HP hardware requiring repair within 12 hours
Other systems being used in production include various Intel-based file servers. There is currently a backup system in place and equipment components could be configured and shipped by the vendor in a short period of time. Full systems will take up to 8 weeks to deliver after the official order has been placed.

4.2 Systems & Operations

This portion of the disaster/recovery plan will be set into motion for ICT Services when an incident has occurred that requires use of the alternate site, or the damage is such that operations can be restored, but only in a degraded mode at the central site in a reasonable time.

It is assumed a disaster has occurred and the recovery plan is to be put in effect. This decision will be made by the Vice Chancellor upon advice from the Chief Information Officer and the COO.

In case of either a move to an alternate site, or a plan to continue operations at the main site, the following general steps must be taken:

- Determine the extent of the damage and if additional equipment and supplies are needed.
- Obtain approval for expenditure of funds to bring in any needed equipment and supplies.
- Notify local vendor marketing and/or service representatives if there is a need of immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- If it is judged advisable, check with third-party vendors to see if a faster delivery schedule can be obtained.
- Notify vendor hardware support personnel that a priority should be placed on assistance to add and/or replace any additional components.
- Notify vendor systems support personnel that help is needed immediately to begin procedures to restore systems software at UFH.
- Order any additional electrical cables needed from suppliers.
- Rush order any supplies, forms, or media that may be needed.
- In addition to the general steps listed at the beginning of this section, the following additional major tasks must be followed in use of the alternate site:
- Notify officials that an alternate site will be needed for an alternate facility.
- Coordinate moving of equipment and support personnel into the alternate site with appropriate personnel.
- Bring the recovery materials from the off-site storage to the alternate site.
- As soon as the hardware is up to specifications to run the operating system, load software and run necessary tests.
- Determine the priorities of the client software that needs to be available and load these packages in order. These priorities often are a factor of the time of the month and semester when the disaster occurs.
- Prepare backup materials and return these to the off-site storage area.

- Set up operations in the alternate site.
- Coordinate client activities to ensure the most critical jobs are being supported as needed.
- As production begins, ensure that periodic backup procedures are being followed and materials are being placed in off-site storage periodically.
- Work out plans to ensure all critical support will be phased in.
- Keep all clients informed of the status, progress, and problems.
- Coordinate the longer range plans with the identified officials, the alternate site officials, and staff for time of continuing support and ultimately restoring the Systems & Operations section.

4.3 Degraded Operations at Central Site

In this event, it is assumed that an incident has occurred but that degraded operations can be set up at the East London Delivery Site. In addition to the general steps that are followed in either case, special steps need to be taken.

- Evaluate the extent of the damage, and if only degraded service can be obtained, determine how long it will be before full service can be restored.
- Replace hardware as needed to restore service to at least a degraded service.
- Perform system installation as needed to restore service. If backup files are needed and are not available from the on-site backup files, they will be transferred from the off-site storage.
- Work with the various vendors, as needed, to ensure support in restoring full service.
- Keep the administration and clients informed of the status, progress and problems.

4.4 Academic Computing

Computing resources from the central site are provided for academic type services to the University. In addition to some batch support at the central site, the majority of this support is over communications lines directly to clients, departments, and various labs across Delivery Sites.

Some general steps that should be taken, in case of a disaster at the central site, are given.

- Determine the extent of the damage and whether additional components can be brought in for present computer systems or whether additional computers need to be brought in.
- Obtain approval for expenditures of funds to bring in added equipment as needed.
- Notify vendor marketing and/or service officials that additional equipment needs to be shipped, with the highest priority, to UFH.

- Notify vendor technical support personnel of the disaster and the need for their assistance.

- Determine if there is a need for any additional electrical cables and order these for immediate shipment from suppliers.

4.5 Use of Alternate Sites

If the central site is destroyed, support of critical academic computing activities will be given from the alternate sites. Additional computer systems will be brought in as needed.

Some steps necessary in this process are listed.

- Determine the priorities of client needs and upgrade computers at the academic labs.

- Set up for operations support.

- Coordinate installing additional equipment and moving support personnel.

- When additional, needed equipment is available, move backup materials from the off-site storage area.

- Coordinate restoring any network communications with Computer & Network Services.

- Coordinate client computing support with clients.

- As production begins, ensure that backup procedures are followed and periodic backups are stored off site.

- Work with the Director of the Center for Teaching Excellence and Academic Computing, the Chief Operating Officer, and clients in coordinating long-range plans for restoring full support by the Academic Computing section.

4.6 Degraded Service from Central Site

If the central academic computing support can be resumed in a reasonable time from the central site, steps will need to be taken immediately to restore these services.

- Determine the extent of the damage and set up procedures to bring in any needed added equipment.

- Determine priorities of client needs and prepare for running at a degraded level of service.

- After the hardware is functioning, perform system installation as needed. If backup files are destroyed at the central site, bring these from the off-site storage area.

- If off-site files are used, replace these at the off-site storage as soon as possible.

- Work with vendors as needed to ensure support is given to restore full service.

- Keep the administration and clients informed of the status, progress and problems.

4.7 Network Communications

There is no redundancy in the computer communications Systems of UFH. UFH has some spare network switches but any other equipment damaged beyond will need to be purchased by ICT services to replace the damaged equipment

In the event of Wide Area Network (WAN) link failure MTN data cards that have been provided on all delivery sites to site Directors or other senior Directors, must be used. This solution will offer degraded performance but is able to work on any device that has a USB port (Desktop and laptop). This use may be commissioned for use by the director in charge at the site or of the division and used until the normal Telkom services have been restored. A usage log is required to be signed by the issuer and user of the device.

This plan does not, at this time, address the problem of a need for redundancy in the telephone switch system. Considerable funds will be needed for an alternate plan in this area in case of a major disaster in the University telephone switch. Providing adequate air conditioning and fire protection are the highest priority.

Since most of the telephone and computer communications lines are buried and in conduits across Delivery Sites, connecting lines to alternate sites and to critical areas cannot be done rapidly.

Some general steps that must be taken in case of a network communications disaster at the central site and/or other parts of the communications network are given.

- Assessment of the damage and an evaluation of steps needed to restore services.
- Assignment of personnel to disaster crews and assignment of tasks. The priority of repairs will be made by the Disaster Coordinator after an evaluation of the critical needs of the University following the disaster.
- If present supplies and equipment on hand are not adequate to restore service as needed, obtain approval for funds needed and contact vendors for priority shipment.
- Coordinate repairs of data communications disasters affecting specific areas of technology support with the recovery team leader of that area.
- Keep the Disaster Recovery Coordinator and team leaders of support areas informed of the extent of the communications damage and recovery procedures being implemented.
- A chart of the communications network at UFH is being developed. When it is completed, a copy of this chart will be placed in the off-site storage areas and onto the Share Point server and periodically updated.

4.8 Personal Computer Recovery Plan

Individual users should plan backups as follows:

Users should save all files created to their network drive as this server backup up is performed using the backup procedure. Any data stored on user machines is the responsibility of the user to save to the network drive, and if required to save to floppy disk, or other storage media. An automated procedure is provided for the replication of data from users machines in the "My Documents" folder to the server.
The programs that are installed on all individual users' computers are created from an image, so it is important to back up data regularly. The policies of the University prohibit users from loading software themselves. The situation should therefore never arise that application or operating system software that may me lost due to a disaster is not backed up on a complete disk image.

4.9 Computer Lab Recovery Plan

In case of an event affecting only a lab, this section of the disaster plan will be executed. For recovery purposes, labs by definition will mean a computer area supporting a number of users as contrasted to an area containing only a few personal computers. An event can occur in an area not defined as a lab; however, it is assumed recovery of services in this situation can be carried out in a routine manner. An area may be considered a lab even if it is in an administrative service area and there are a large number of personal computers involved.

A disaster will be declared in a lab when a large portion of the units in the lab are affected to the extent that recovery in that area in a reasonable time with normal procedures is not possible.

General steps that will be followed in recovery of a lab are listed. The team leader of the computer area with support duties over the lab affected will assume prime responsibility in the recovery process.

- Determine the extent of the damage in the lab and whether alternate lab services will be needed while recovery is taking place.
- Obtain University approval for any funds needed to replace equipment and supplies.
- Determine whether adequate equipment is available on Delivery Site, either from the Delivery Site Store or other areas, to restore even partial services in the lab affected.
- Coordinate recovery of the center with Computer & Network Services if communications lines are involved in the lab.
- If alternate services are to be provided for clients of the lab, coordinate activities between groups affected.
- Keep the Disaster Coordinator informed of the status of the lab and the recovery process.

5.0 Emergency Procedures

In case an incident has happened or is imminent that will drastically disrupt operations, the following steps should be taken to reduce the probability of personal injuries and/or limit the extent

of the damage, if there is not a risk to employees. Similar steps should be followed, where appropriate, in incidents occurring in a satellite center.

- An announcement should be made to evacuate the building, if appropriate, or move to a safe location in the building. As a preparation for a potential disaster, all Information Technology Division personnel should be aware of the exits available.
- If there are injured personnel, ensure their evacuations and call emergency assistance as needed.
- If the computers and air conditioning have not automatically powered down, initiate procedures to orderly shutdown systems when possible.
- When possible and if time is available, set up damage limiting measures.
- Designate available personnel to initiate lockup procedures similar to last shift procedures.

5.1 Alternate Computing Services Facility (DR Site)

A Disaster Recover system has been established in East London for the Document Management System (DMS) area where two HP servers are located. The servers are in a configuration to ensure maximum redundancy for the DMS system. One Virtual server Cluster is installed in the server room at 50 Church Street and the other in the basement of Gasson Centre. Gasson Centre is linked to the 50 Church Street Street site by underground fiber cables to ensure that lightning and other environmental disturbances are minimized.

5.2 Off-site Storage

All central file backups are made on magnetic tapes or other compact media using an appropriate backup strategy and stored in a safe on the UFH Delivery Site.
The ICT Services employees have access to keys both to the exterior doors and to the room where tapes are stored. A copy of the full backups is also stored in the safe adjacent to room 124 Gasson Centre.

5.3 Vendor Contact list

5.3.1 HP - HP server for ITS that run in the VMWare Environment
---

ELANDRE SCHONKEN – DIMENSION DATA, EAST LONDON: 072 258 9577

5.3.2 Telkom – Telephone systems and Data Circuits

XOLANI TEBELE – TELKOM CLIENT SERVICES: 081 317 5277

5.3.3 Tenet - Internet service provider

MR. DUNCAN GREAVES – CEO TENET: 082 555 5719

5.4 Emergency call list for ICT Division

CHIEF INFORMATION OFFICER – Dr. C.P. Johl Cell 079 520 4414 Cell, Fax 086 625 7364
ICT OPERATIONS MANAGER ALICE (acting): Mr. Jama Mbatani, Cell, No 072 023 9193
ICT ENTERPRISE MANAGER EAST LONDON (acting): Mr. Lusanda Matyunjwa 076 866 8732
ENTERPRISE ADMINISTRATOR: Mr. Nico Lambrechts, 083 459 7546
NETWORK ADMINISTRATOR BHISHO: Mr. Agboola Teru, 076 141 7228

5.5 Emergency call list for Physical resources

5.5.1 Director Properties and Services

The acting Director of Properties and Services Mr. Langa Mbude 082 054 4282is contactable on his Cell phone 082 084 5978 all hours unless otherwise notified. He manages the security division and all building related services. Mr Kaizer Dlemnango is the alternate contact on 076 752 0896

--
C.P. Johl - IT Division - UFH - East London
mailto:cjohl@ufh.ac.za; cell:+27 79 520 4414; fax:+27 86 625 7364 (fax-to-email)

Signed:

Dr. C.P. Johl Chief Information Officer Date: 2 March 2016

Mr. L. Mbude acting Director Properties and Services Date: 12/07/2016

Dr. M. Tom Vice Chancellor and Principal Date: 12/07/2016