CAPE COAST TECHNICAL UNIVERSITY

DISASTER RECOVERY PLAN

CCTU P NO. 29

CAPE COAST TECHNICAL UNIVERSITY

GAZETTE

DISASTER RECOVERY PLAN

April 3, 2025
CCTU P NO.29

PUBLISHED BY THE DIRECTORATE OF PUBLIC AFFAIRS

TABLE OF CONTENTS

Forward

The Part 1 section 1 of the first schedule of the Technical Universities Act, 2016 (Act 922) as amended converted qualified polytechnics to Technical Universities to provide higher education in engineering, science and technology based disciplines, technical and vocational education and training, applied arts and related disciplines.

The Cape Coast Technical University is a national institution with a mandate to provide higher education guided by the Technical Universities Act, 2016 (Act 922) as amended. As a national institution, the University globally serves several interest groups and stakeholders. By extension the University exist to train for the future requisite professionals that will directly or indirectly impact the society.

The University recognizes the future is unpredictable. Therefore the mandate to train requisite professionals for future needs usually require the realization of an approved strategic plan. The ability to see through the future and take calculated risks in a way that does not jeopardize the interests of its stakeholders is also key factor to the successful achievement of this mandate. Hence the need for a Disaster Recovery Plan (DRP) that sets out the University's objectives and strategy for Disaster recovery strategies. It is a formal document created by the University and contains detailed instructions on how to respond quickly to any unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events including pandemics and

also regaining access and functionality all strategic and operational to asset for business continuity purposes.

As a national institution, The Governing Council is the highest decision-making body of the University.

The Governing Council and the management are responsible for a Sound control environment with relevant control activities that will enable the University to anticipate and respond quickly to changes in the work environment, as well as make informed decisions under any conditions of uncertainty.

It is for these and other reasons that the governing council shall constituted a Committee to develop a risk management Plan, Risk management register, Disaster Recovery and Business Plan for the University.

The DRP shall serve as a guide to Management and Staff in integrating risk management framework into the University's' operations in a more structured way that allows for the manifestation of its Vision, Mission, Objectives and Core values. This Plan when approved shall provide a systematic way of assessing, managing and responding quickly to both the strategic and operational Disasters at all levels of the University.

The Governing Council on behalf of the Government through the Mother Ministry shall presents and approve this Plan to guide and assist management in responding quickly to all disaster with minimum or zero catastrophic losses.

STATEMENT OF VISION, MISSION, CORE VALUES AND SWOT ANALYSIS

Vision Statement

Our vision is to be a leading technologically innovative and entrepreneurial Technical University with a reputation in green and clean energy technologies.

Mission Statement

Our mission is to provide quality technical, vocational and entrepreneurial education that inspires learners to be creative and driven towards technology-based and sustainable solutions for communities and industries within the country and the sub-region.

Core Values In pursuing its vision and mission, Cape Coast Technical University will be guided by these core values: Innovation, Creativity, Professionalism, Integrity, Discipline, Respect for all, Team spirit, Service to community.

Core Functions

The following core functions will guide the institution in realizing its vision and mission: Teaching, Research and Innovation, Entrepreneurial Skills Development, Consultancy Services, Community Engagement

Environmental Scanning

Cape Coast Technical University is positioning itself as a leading University based on a deep integration of technical skills, innovation and entrepreneurship, to realize practical solutions for national development. As a technical university, CCTU's core mandate is to provide higher education in applied sciences, engineering and technology-based disciplines. However, in Ghana, the proportion of students who are willing to pursue technical and vocational programmes is generally small, thus making it difficult for technical universities to achieve enrolment targets that will generate adequate revenues to make them competitive. The main reason for the poor enrolment is the negative perception about technical and vocational education created by a lack of government support for Technical and Vocational Education and Training (TVET).

Introduction

Staff and students of Cape Coast Technical University (CCTU) of late usually or mostly rely heavily on use of the available Information Technology (IT) infrastructure and Network services (i.e. use of Desktop computers) to accomplish their work. For this reason management also now considers IT and Systems Automation as an integral part of the working and learning environment. As a result of this practice, IT services are now being considered a critical component in the daily operations of CCTU, requiring a comprehensive Disaster Recovery Plan that is structured to provide strong assurance that the University's services can be re-established promptly and completely in the event of a disaster of any form or magnitude.

Response to and recovery from a disaster at a University shall usually be managed by the University's Risk Management Committee (RMC). The actions of the RMC are governed by the University's Risk Management Plan and Charter.

This Recovery Plan is set to presents the requirements and the steps that shall be taken in response to and for the recovery from any disaster that may affect the services of the University, 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.

The University this regard is currently improving its IT management services for both data Input and Storage centers to facilitate prompt recovery of operations.

This Plan shall be reviewed and be updated annually by the RMC together with the staff of IT management services and approved by the University through the Academic Board.

The Cape Coast Technical University acknowledges the fact that, factors within its operating environment both internal and external have the capacity to pose numerous risks, which have the potential to disrupt the achievement of its strategic and operational objectives. The University therefore, in order to mitigate this, intends to use the ISO **31000 Enterprise Risk Management Framework (RMF)** to make informed decisions and enhance the achievement of its strategic goals and operational objectives.

Plan Statement

This Plan forms part of the University's internal control measures and corporate governance arrangements, intended to summarize the view of the University Council with regard to its Disaster Recovery management philosophies. The DRP comprehensively explains the consistent actions that must be taken before, during, and after a natural or man-made disaster so that the entire team can take those actions. The University considers Disaster Recovery Management (DRM) as a fundamental activity to good management practices and a very significant aspect of corporate governance. As such, DRM shall be an integral part of the decision-making and also, shall be incorporated within the strategic and

operational planning processes at all levels across the University. This will be achieved through the following:

a) Continual assessments of all new and ongoing ventures and activities, including projects, processes, systems and commercial activities to ensure that they are all aligned with the University's Disaster recovery objectives.

b) Identifying, analyzing and reporting to the appropriate management levels (DR Unit), any elements or signals of disaster and the possible or probable losses that may be arising from the assessments.

c) Maintenance of a Backup register for all key strategic and operational information by the University's DRM Unit.

d) Maintenance of adequate Backup devices and registers by all Schools, Directorates, Departments, Administrative Sections and Units.

e) Provision of all staff with adequate education, guidance and training on the principles of Disaster recovery plans and their responsibilities to implement them effectively when and where necessary.

f) Regular review and monitoring of the effectiveness of the existing DRM process, including the development of an appropriate DRM culture.

Plan Objective

Contingency and disaster recovery management refers to the criteria and procedures used to guide management and all technical staff in the recovery of all asset and liabilities and respective material information operated by the University and its networked facilities in the event that a disaster destroys all or part of the CCTU.

The establishment of this Plan is necessary to the facts that, the Public Financial Management (PFM) 2016, Act 921 and its related regulations place emphasis on the need for establishment of effective risk management practices and good corporate governance principles that aimed at improving efficiency and effectiveness of State-owned organizations.

It is on this basis that the University's governing council and management has developed this Disaster Recovery Management Plan (DRMP). The University is committed to the management of all disasters and exposures as an integral part of its operations, by implementing strategies that seek to minimize threats from these exposures and enhance opportunities to the achievement of its goals and objectives.

The administration of this Plan is to ensure and also allow the management of the University to:

a) Have level of confidence in achieving its stated mandate and objectives;

b) Manage and reduce the effects all disasters at all times to tolerable levels that allow for business continuity;

c) Align DRM with the University's objectives (as set out in the Strategic Plan)

d) Assign responsibility desks for DRM at every department within the University especially with in ICT and Quality Assurance, Works and Development, Finance, Human Resource, Legal and the Academic affairs.

e) Appraise and manage the consequences all disasters in a systematic, structured and timely manner, in accordance with best practice National Disaster Management team;

f) Collaborate with the following State Agencies; National Disaster Management Organization, Fire Service, Environmental Protection Agency, Information Security and Data Protection Agency, etc. to provide education, awareness creation and sensitization of DRM processes to all stakeholders of the University.

g) Provide adequate DRM training to staff at all levels of the University especially the Security and Maintenance Section.

h) Formalize and communicate a consistent approach to DRM for all University activities

i) Make informed and environmental friendly decisions; and

j) Strengthen internal control and preventive procedures.

Scope of the Plan

This Plan covers all activities of the University that are critical for business continuity. However due to the uncertainty regarding the

magnitude of any potential disaster on the campus, this Plan shall mostly address the recovery of systems under the direct control of the Department of Information Technology. Indeed the University fully recognize the facts that the total recovery of these systems themselves shall be beyond the scope of this document and also the ability of the IT department. However this Plan is being put in place with all its underlining strategies to address and restore connectivity and also integrate services within the University system for successful business continuity.

The contingency and disaster recovery plan is composed of a number of Sections that will continually monitor and document all strategic and operational resources and procedures (recovery tasks and an organizational structure for the recovery process) to be used in the event that a disaster occurs at the University. This includes the following major areas:

- Desktop equipment, labs, classrooms
- Data networks and telecommunications (wired and wireless networks, file services)
- ELearning & Library management system
- Emails & Cloud Management (Google Apps / cctu.edu.gh)
- Student Management Services
- Finance and Accounting software management systems

Effective DRM principles shall therefore become part of the routine management in the University and will include continuous assignment responsibilities like:

- ✞ Incident Response Unit (IRU) which shall be responsible for planning and responding to all IT incidents, including cyber-attacks, systems failures, and data breaches to enable the University to quickly detect and halt attacks, minimizing damage and preventing future attacks of the same type.
- ✞ Disaster Impact Assessment and Declaration Unit (DIADU) which shall be responsible for a making impact assessment and issue a formal statement within its assessment jurisdiction that a disaster or emergency exceeds the response and/or recovery capabilities or not.
- ✞ Post incident Review Team (PIRT) which shall be responsible for bring people and teams together to discuss the details of an incident: why it happened, what impact it had, what actions were taken to resolve it, and how the team can prevent it from happening again.

This Plan and its associated explanatory guidelines shall be adopted by Council and be applied throughout the University. This Plan shall also applies in full to all our IGF Centers with formal approval to be commercialized and operate as semi-autonomous entities.

Disaster Management Assumptions and Culture

The Cape Coast Technical University exist to serve and impact the lives of several interest groups and stakeholders. These services and its impact shall either be direct or indirect depending on the geographical location and other environmental factors of its interest groups and stakeholders.

Business activities and day-to-day operations of the University mostly resides on the computers and the available networks systems. Today you can find computer systems in every department on campus with workstations and servers that are linked together by a sophisticated network that provides communications with other systems across campus and around the world. For this reason, most essential functions of the University currently depends on the availability of this network systems. Consider for a moment the impact of a disaster that could probably prevents the use of the existing the systems to process Student Registration, Payroll, Accounting information, University Healthcare systems, Graduated student data and etc. for even a week or two. It is hard to estimate the damage that CCTU might incur and even cause others.

This disaster response and recovery plan shall be based on the following assumptions:

Real-time resource provision: Once an incident covered by this plan has been declared a disaster, the appropriate priority will be given to the recovery effort and the resources and support required shall be available.

Human safety priority: The safety of students, staff, and faculty members are of primary importance and shall be safeguarded and be rescued first before the safeguarding other concerns including hardware, software and other recovery needs.

Systems flexibility and adjustment requirement: Depending on the severity of the disaster, the University Management with the Council's approval shall require all affected Directorates, Departments, and Sections to modify their operations to suit any changes in physical location system performance, and resource availability until a full recovery is completed.

Departmental Specifics: The Risk Management Committee and ICT Directorate shall encourage all other departments to have departmental Risk assessment register, Contingency & Recovery plans and Business Continuity Plans for their operations,

Revision & Update: The content of this plan shall at all-time be ready for modification especially in the event of an unusual or unforeseen substantial deviation and circumstances.

The said circumstances shall always be determined by the specific Disaster Recovery Teams under the guidance and approval of the Incident Commander and Incident Command Team.

Auditing disaster recovery plans and systems

Special Audit Team comprising staff of Internal Audit, ICT, Security Section and representations from the specific Unit shall regularly audit

the DR plan to reflect changes in the University services and ensure that those tasked with bringing these services back up are working with the correct information.

Changes to the University services such as IP address, VLAN, Administrator access and firewall settings should be updated as soon as these changes are made to the system audited and certified.

It is also important to audit access to the DR plan and its related documents to reflect changes in staffing, contact information, and administrative access.

It is obvious that students and faculty rely upon these systems for instruction and for research purposes, all of which are important to the well-being of the University as well as its surrounding Communities and Stakeholders.

Without adequate planning and preparation to deal with such an event, the University could lose its computer information and administrative systems.

The University in this regard is committed to developing a consistent and appropriate DRM programs and assurance cultural practices that seek to ensure that the key stakeholders (including staff, students, other service providers, contractors and surrounding communities) are recognize in its commitment to Contingencies and Disaster recoveries responsibly.

The established DRM culture shall also in itself establish a Management Framework that allows for effective operationalization of all other relevant policies including the; Strategic plan, Risk Management Plan,

Risk Management Charter, Disaster recovery plans, Bussiness Continuity Plans, Backup services and assurance Plan, Staff development and capacity building policies, Business Operations & Administrative Manuals, Asset management and embossment Plan, Asset register and Risk Register.

Departmental disaster recovery planning

The purpose of this document is to instruct and help all departments form a disaster recovery plan. Many services hosted by the departments are key in conducting daily university business.

Departmental disaster recovery planning involves the process, policies, and procedures that enable delivery of critical technical services to the department in the event of natural or man-made disaster. Departmental Disaster recovery (DDR) shall also form an integral part of the overall business continuity program.

Backup Procedures

The Office of Information Technology is responsible for backing up regularly all servers and other storage devices. The backup media for each of these systems shall be relocated to an off-site storage area where there is a high probability that the media will survive in the event a disaster strikes.

The regular backup procedures shall include:

1. The University shall procure for this purpose automated backup software

2. Server backups shall be performed every business night, including holidays.
3. Backups performed on weekends (especially with regards to unique assignment) shall be kept for a month before recycling.
4. Backups shall be secured and monitored by a full time Confidential IT staff member(s).
5. Backups shall be performed using automated backup software.
6. Backup failures will be reported to the Director of Information Technology and the Registry for actions to be taken quickly to fix the problem.
7. Backups will always be performed before upgrading or modifying a server.

Recovery Preparations

A critical requirement for disaster recovery is ensuring that all necessary information is available to assure that hardware, software, and data can be returned to a state as close to "pre-disaster" as possible. Specifically, this section addresses the backup and storage practices as well as documentation related to hardware configurations, applications, operating systems, support packages, and operating procedures.

Application of Recovery Information

Information necessary for the recovery and proper configuration of all application software located on the central servers is critical to assure that

applications are recovered in the identical configuration as they existed prior to the disaster. Detailed information on critical central applications will be documented in our monitoring system and infrastructure website. The infrastructure staff is responsible for keeping the software inventory up to date.

Desktop Equipment Recovery Information

Information necessary for the recovery and proper configuration of all desktop computers and printers supported by Information Technology Services is critical to assure that client systems can be restored to a configuration equivalent to pre-disaster status. Detailed information on client systems (both PC and MAC) is documented in our monitoring system, infrastructure website, and Microsoft System Center Configuration Management database. The infrastructure staff is responsible for keeping the hardware inventory up to date.

Incident Occurrence

Upon the occurrence of an incident affecting the IT services of the University, the Vice Chancellor and the Register shall be notified by campus security or other individual presents. Personnel reporting the incident will provide a high-level assessment as to the size and extent of the damage.

Disaster Recovery Processes and Procedures

The Disaster Recovery processes and procedures shall include:

Emergency Response: The requirement for Emergency Response Team (ERT) involvement and the membership of the ERT shall be dependent on the size and type of the Crises.

Examples of situations which will normally result in the involvement of the ERT shall include:

- Severe structural damage to the facility where personal safety is in question, and where analysis must be completed to assure the building is acceptable for access. This shall include, but not limited to, damage from a flood or cyclones.
- Environmentally hazardous situations such as fires, explosions, or possible chemical or biological contamination where the situation must be contained before allowing for building occupancy.
- Flooding or other situations which may pose the risk of electrical shock or other life-threatening situations.

Examples of situations which will normally not result in the involvement of the ERT include:

- Major system/hardware failures that do not pose a hazard to personnel or property.
- Utility outages (electrical, etc.) which are remote to the datacenter being affected.

Activation of the Emergency Plans

The Vice Chancellor of the University or, in his absence, the Pro-Vice President or the Registrar shall declares a "state of emergency" whenever there is a threatened or actual condition of disaster or extreme peril that cannot be managed by ordinary campus procedures. A "state of emergency" may also be declared in response to heightened national alerts. The Recovery Coordinator shall initiate the notification process and the response procedures for the primary response to campus emergencies.

For pre-planning or for short-term emergency operations, an Emergency Operations Center (EOC) shall be established in the University Conference (Meeting) Room for the coordination of all communications and actions. However for expected long-term emergencies, the EOC will convene in the lower offices of School of Business. The Coordinator will notify all the University emergency response personnel to activate the emergency response programs.

The emergency response personnel will then direct all University faculty, staff and students about the correct response procedures to the particular emergency which may include the designation of a meeting location for emergency personnel. Unless designated otherwise, the University Emergency Response Team will meet on the ground floor of the located Area or building to receive their instructions.

The Director of Public Relations or a designee will respond to media inquiries, issue press releases, and designate one central location for the

meeting of media personnel with University representatives for the dissemination of information.

The plan shall be activated upon such a declaration in the following sequence:

- If the emergency occurs during normal business hours, all designated management personnel shall report to the EOC as soon as possible.
- If the event occurs after normal business hours, key management personnel their emergency response team shall be called back to the campus.
- A list of key faculty and staff members with appropriate phone numbers, shall be maintained by Campus Security and Safety Officers.
- If the disaster is so large as to unquestionably have a profound impact on the campus, all key management members and staff shall be instructed to return to campus as soon as possible.

Emergency Plans: This Plan is designed to capture and activate Emergency Plans to the following schedule of unplanned events:

1) National Threat or Terrorism Plan: Globally institutions have been living with the threat of incidences of terrorist attack. It is advised that adequate and strategic preparedness to this may lessen the damage to property and the loss of life. The University in this regards shall:

- Ensure University Emergency Response and Disaster Recovery Plan is current and disseminated to all staff and students.

- ✞ Train security personnel on proper system managing prompt response to unplanned incidence.
- ✞ Develop heightened security measures that provides real-time response to National Security Advisory System.
- ✞ Monitor the alert status of the National Security Advisory System.

2) **Emergency Fire Plan (EFP):** Fire is the most common of all hazards. Every year emergency fires cause thousands of deaths and injuries and billions in property damage. Adequate prevention and planning could reduce to the minimum injuries and losses caused to lives or properties.

The University in this regards apart of its emergency plans will:

- ✞ Meet with the fire department to discuss operations and identify the processes and materials that could cause or fuel a fire or contaminate the environment in a fire.
- ✞ Have all facilities inspected for fire hazards and insure them with relevant fire codes and regulations.
- ✞ Ensure each building and vehicle has a fire alarm, smoked detectors or notification system insulted to warn and alert occupants of fire danger.
- ✞ Have an active insurance Plan for University and Keep a copy of the University insurance Plan on hand at all times.
- ✞ Distribute fire safety information to employees and students sensitizing them to be aware of:

a) How to prevent fires in the workplace or at residential halls.

b) How to contain a fire.

c) How to evacuate the facility.

d) Where to report a fire

e) The safety ways to make, maintain and use fire

- Instruct personnel to use the stairs - not the elevators - in a fire.
- Instruct them to crawl on their hands and knees when escaping a hot or smoke-filled area.
- Conduct evacuation drills. Post maps of evacuation routes in prominent places. Keep evacuation routes, including stairways and doorways, clear of debris.
- Assign a Building Emergency Coordinator for each building to monitor shutdown and evacuation procedures.
- Place fire extinguishers in appropriate locations.
- Train employees in the use of fire extinguishers.
- Install smoke detectors. Check smoke detectors for proper operations as required.
- Ensure that key personnel are familiar with all safety systems.
- Install closed-circuit television to provide video surveillance and have the connected key Officers' phones.
- Identify and mark all shutoffs so that electrical power, gas, or water can be shut off quickly by responding personnel.

3) Flood and Flash Flood Plan: Globally floods are among the most common and widespread of all natural disasters of which Ghana is not an exception. Most communities in this region experience some degree of flooding after spring rains, or heavy thunderstorms, most floods develop slowly over a period of days. Flash floods, however, are like walls of water that develop in a matter of minutes. Flash floods can be caused by intense storms or dam failure. Although the University sits on high ground, we will however remain committed to:

- ✞ Review the community's emergency plan.
- ✞ Establish warning and evacuation procedures for all University the facility.
- ✞ Make plans for assisting employees who may need transportation.
- ✞ Inspect areas that may be subject to flooding during heavy or prolonged rains.
- ✞ Identify any equipment that can be moved to a higher location.
- ✞ Have on hand information on daily Weather updates.
- ✞ Take precautions and be prepared to go to higher ground. If advised, evacuate immediately.

4) Cyclone Plan: Cyclones are incredibly violent local storms that extend to the ground with whirling winds that can reach 300 miles per hour. Spawned from powerful thunderstorms, cyclones can uproot trees and buildings and turn harmless objects into deadly missiles in a matter of seconds. Damage paths can be in excess of one mile wide and 50 miles

long. They occur with little or no warning. The University having this in mind will:

- ✞ Review the local cyclone warning system and develop a campus cyclone warning system to notify faculty, staff and students of need to seek shelter.
- ✞ Be prepared to take shelter and take shelter immediately
- ✞ Be prepared to shelter faculty, staff and students.
- ✞ Buildings that can serve as cyclone shelters will be identified and marked as such.
- ✞ The best protection in a cyclones is usually an open area and field.
- ✞ If an open area and field is not available, the following areas will be considered:

a. Small interior rooms on the lowest floor and without windows.

b. Hallways on the lowest floor away from doors and windows.

c. Rooms constructed with reinforced concrete, brick, or blocks with no windows and a heavy concrete floor or roof system overhead. .

5) Technological Emergency Plan: Technological emergencies include any interruption or loss of a utility service, power source, information system, or equipment needed to keep the facility in operation. To minimize loss of operations, the University will:

- ✞ Identify all critical operations, including the following:
    - **a.** Utilities including electric power, gas, water, hydraulics, compressed air.

b. Alarm systems, elevators, lighting, heating, ventilation, air conditioning systems, and electrical distribution systems.

c. Communication systems, both data and voice computer networks.

✞ Develop a plan for backup power sources.

✞ Establish a Cold Site location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is usable.

✞ Maintain offsite backup storage for recovery of lost data.

✞ Establish preventive maintenance schedules for all systems and equipment.

6) Hazardous Material Emergency Plan: Hazardous materials are substances that are either flammable or combustible, explosive, toxic, noxious, adhesive, corrosive, oxidizable, an irritant or radioactive. The University will:

✞ Identify and label all hazardous materials stored, handled, produced and disposed of by the University, after following required safety protocols and government regulations that apply to the storage and use, and also obtain material safety data sheets (MSDS) for all hazardous materials on the campus.

✞ Ask the local fire department for assistance in developing appropriate response procedures.

- ✞ Train employees to recognize and report hazardous material spills and releases.
- ✞ Train employees in proper handling and storage.
- ✞ Establish a hazardous material response plan that will further:

i. Establish procedures to notify management and emergency response teams of an incident.

ii. Establish procedures to warn employees of an incident.

iii. Establish evacuation procedures.

a. Organize and train an emergency response team to confine and control hazardous material spills in accordance with applicable regulations.

b. Identify other facilities in the area that use hazardous materials and determine whether an incident could affect the University.

c. Identify highways and other access road near the University used for the transportation of hazardous materials and also determine how a transportation accident near the Campus could affect operations.

7) Emergency Notification Plans and Procedures: For most emergency or disaster situations, the following notification procedures shall be followed:

a. Fire alarms and flashing lights will be activated to notify occupants of buildings in which an emergency or disaster has occurred and evacuation is required.

b. During work hours, faculty, staff and students will be notified by campus e-mail and campus radio broadcast of emergency situations or pending emergency situations, such as severe weather or national emergency.

c. Supervisors will ensure that all employees in their area have read their e-mail and are aware of the situation.

d. Faculty will ensure that all students in their classes are aware of the situation.

e. The Dean of Student Affairs shall be responsible for ensuring that students residing in the residence halls are aware of the situation.

f. Campus radio messaging shall be coordinated by the Hostel Warden, Director of Public Affairs Department of Campus Safety and Security, and ICT.

g. After work hours, faculty, staff and students will be notified through the Campus radio station and or by campus e-mail on the status of the University and of any emerging signal of disaster, such as in the case of severe weather or national emergency. The notifications will be coordinated by Campus Safety and Security Personnel.

h. Supervisors of the various Units and Sections will develop a plan to contact employees to ensure that they are aware of the status of the University periodically.

i. The Dean of Student Affairs is responsible for ensuring students residing in the residence halls are notified about the status of the University. In the case of a prolonged emergency or disaster, the Director

of ICT, in conjunction with the Director of Public Relations, will coordinate to announce the status of the University on the website.

8) Emergency Evacuation Procedures Emergency situations that call for evacuation of classrooms and buildings will be announced by the emergency fire alarm horns and visual alarm system (in addition to alarms, flashing lights are installed in some buildings). The University is to procure and install essential gargets. When these alarms sound or are seen, all persons should immediately leave the building. The following guidelines should also be observed at all times:

- Treat all alarms as if they warned of real emergencies.
- If it is found that the alarm is not being heard and/or seen in all buildings, continue with proper and complete evacuation of the building(s) in which the alarm is heard and/or seen.
- Use appropriate exit – do not use elevators.
- Exit the building following the posted routes in the classroom and /or office complex.
- Alternate exit routes shall also be indicated on the posted routes should there be a blocked exit.
- Assist people with disabilities.
- All persons should allow for the presence of persons with disabling conditions and provide assistance if needed.
- Always ask before assisting to make sure assistance is needed and done as safely as possible.

- Check all areas on your floor and/or in your building to be sure of your evacuation success.
- All faculty and staff are expected to help in ensuring that all areas, including the, restrooms, and offices are evacuated.
- Persons who do not have a class group or laboratory to take care of should be particularly alert to the need to assist in clearing all areas.
- Close (but do not lock) windows and doors.
- Remember that closed windows and doors can reduce the spread of fire and/or hazardous materials and fumes.
- Turn off laboratory gases, exhaust fans, etc.
- Turn off all sources of fuel and oxygen (air) that might feed a fire or spread fumes.
- Call fire department or emergency services and campus safety.
- The first person(s) to discover the emergency is (are) responsible for calling the Chief Administrator of Campus Safety and Security who will contact the local fire department or emergency services.
- Be calm and carefully give all needed details of the specific location, type of emergency, your name, etc.
- The same Contact numbers should be called for emergency medical care service and pertinent information given.
- Make sure campus safety and maintenance personnel are aware of the alarm.
- If you do not see definite indications that Facilities personnel are aware of the alarm, notify the Facilities directly through either telephone

call, send someone, or go yourself to ensure that Campus Safety and Facilities are aware of the alarm. Give them your name and the name of the building where the alarm is occurring.

9) Emergency Evacuation for Students who have Mobility challenges (Wheelchair).

The university shall from now establish an operational Office for Disability Services under the office Counseling & Consultation Unit). In the event of any condition that may require emergency evacuation for Students with Disabilities or Mobility Impaired, the University has the following procedural arrangements made;

- If a student is on a floor in a multi-story building with no accessible outside exit or in a multi-story building where the accessible exit(s) is blocked, the said student should go to the designated wait area for assistance. If assistance is unavailable, the student should ask someone leaving the building to notify the Emergency Coordinator of the location and the need for assistance.

Lifting Wheelchair Students

If a student needs to be lifted and carried up or down a stairwell, the student should know the safest way to proceed and should be asked how he or she prefers to be lifted and carried. This is because most electric wheelchairs are heavy to be lifted and may need to be left behind.

- Physically challenged persons who can walk independently with little or no assistance may wait until heavy traffic has passed and then proceed.
- While waiting in a designated wait area for assistance, the victim can equally call to notify the Emergency Coordinator of the location for assistance.
- Physically challenged persons (hearing impaired). Campus buildings are to be equipped with fire alarm strobe lights to assist if a student needs to be alerted of an emergency situation and an interpreter is not around.

Visually Challenged Students

Most visually impaired students are usually familiar with their immediate surrounding and frequently traveled routes but may need assistance navigating an unfamiliar and/or crowded route out of the building.

- The person offering assistance should offer an elbow and guide the student out of the building, communicating as necessary for a safe evacuation and when you reach safety, orient the person to the location.
- Note, Students with disabilities who have evacuation concerns and issues should:

i. Meet with the Coordinator of the Office of established Disability Services (Counseling & Consultation Center,).

ii. Familiarize self with campus accessibility.

iii. Be prepared to communicate needs.

Universal Emergency Recovery Functions:

At critical points of emergencies and disaster recoveries, it is and shall always be a mandatory requirement that all Responsible Units and departments throughout the campus shall to provide the following basic emergency functions:

1. Emergency Communications:

The Campus Security and Safety office assisted by office Public Relations shall be responsible for the general oversight of emergency communications including:

a) **Establishing an Emergency Operation Communications Center**. During emergencies, Campus Security and Safety shall establish and maintain communications with the City Authorities Emergency Management (i.e. Fire Service, NADMO, Police and etc.) as well as maintaining communication on campus.

b) Identifying the total number of portable video garget available at that will facilitate assignment coordination and use them during an emergency.

c) Identifying the number of cellular phones available at the University.

d) Coordinating with ICT section to establish priority areas of information storage, and to maintain a UPS (uninterrupted power supply) for the Storage Centre's.

e) Coordinating with campus electricians to use portable generators to maintain sustainable power supply systems.

f) ICT is responsible for Setting up “hot lines” for emergency calls within Campus.

g) The ICT office is responsible for ensuring the protection and recovery of computer equipment and data information.

h) Key ICT personnel who are part of the disaster and recovery team and will:

1. Restore and maintain telephone communication at the University.
2. Ensure the protection and preservation of computer equipment. In particular, any magnetic storage media (hard drives).
3. Survey the disaster scene to estimate the amount of time required to put the facility and technology operations back into working order.
4. Relocate to the Cold Site, a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored.
5. Ensure that work begins to repair or rebuild the primary site.
6. Make necessary arrangements with vendors to quickly provide replacements for the resources that cannot be salvaged.
7. The University will develop emergency procurement procedures to quickly place orders for equipment, supplies, software, and any other needs.
8. Reassemble salvaged and new components at the recovery site.

9. Restore data from backups stored in locations off-site. Backups can take the form of, disk drives, and other storage media.

10. Early data recovery efforts shall focus on restoring the operating system(s) for each computer system.

11. **Restoration of Applications Data:** The ICT Recovery staff shall coordinate with users and departments (e.g., the application owners). The Director of Information Technology and staff will develop a detailed response and recovery plan that will ensure restoration of operations as quickly as possible with the latest and most up-to-date data available.

Damage Assessment: In the event of an emergency or disaster in which buildings may be damaged; an assessment must be made prior to further use. Management of the affected Facilities shall be responsible for the general oversight of damage and damage assessment inspections. Safety assessment forms shall be given to occupants of these facilities to be completed and forwarded to the Facilities Management representative of the Disaster recovery and Risk Management Team.

Assessments Inspection and Damage stickers:

Inspection stickers of different colours representing different degrees of damages shall be developed for this assessment. Whether or not there is damage, each building shall be posted with inspection stickers. Assessment surveys of all building damage will be initiated with a focus on utility lines disagreements and structural damages sustained by buildings, as well as possible release of hazardous material. Immediate

assistance shall be given to injured persons as necessary. Final damage estimates shall be coordinated and communicated to the Disaster recovery and Risk Management Team.

Building Emergency Coordinators:

The University shall collaborate with the leadership of the Students Representative Council (SRC) to have and trained a strong Cadet force and Red Cross society on campus who shall assist the Disaster Recovery and Risk Management Team during emergencies. Building Emergency Coordinators (BEC) shall be formed from these Teams with a sole responsibility to clear all persons out of structures as soon as possible. All persons shall move toward the designated Disaster Evacuation Areas. Each building shall be prioritized in the emergency plan from highest to lowest risk. The Scheme for ranking or prioritizing shall be based on the building's age, number of people normally occupying the structure, safety designation, containment of hazardous materials, and specific use (student housing, medical care facility, etc.) Buildings will be surveyed on that priority basis. All buildings on campus will be evaluated by independent evaluation teams outside to ascertain the degree of damage that has been sustained. Initial building entry shall only to be made by management and employees of the floors or structural engineers who are trained to assess the degree of damage from an engineering perspective. They will:

a) Examine the entire outside of the structure and also check the ground in the general area of the structure for fissures (Cracks), bulged or swollen ground, or sign of slope movement.

b) Only enter a building only if the structure cannot be viewed sufficiently from the outside or when there is a suspected or reported problem such as gross nonstructure distress (e.g., fallen ceiling, or badly damaged partitions visible from the outside). Do not enter obviously unsafe structures.

c) Evaluate the structure quickly without going into a detailed investigation. When a building's structure is questionable, it should be scheduled for a more detailed evaluation.

d) Make sure exits are clear.

e) Tag each building with a coloured placard placed on each main door indicating the degree of damage that has been determined. Three categories or colours of signs shall be used:

- **RED** – Building is unsafe, indefinitely- DO NOT ENTER
- **YELLOW** – Limited entry only to designated personnel
- **GREEN** – Safe to re-enter

Buildings that have been seriously damaged or contaminated with hazardous material spills shall be posted with yellow. Additionally hazardous warning barrier tapes shall be hang on both yellow and red coloured building by team members. Doors will be secured to prevent re-entry by unauthorized personnel. All other structures shall be coloured or coded appropriately after the initial inspection process.

The University also takes recognition to the facts that emergency or disasters has the capacity to pose threats to various utility lines (e.g., gas, water, and power) or may cause them to be severed or severely interrupted. In this management shall dispatch personnel to inspect, examine, or shut off valves controlling gas, water, or power.

Special Treatment Protocols: The following treatment protocols have been outlined to cater for emergencies like;

- **Gas Leakages;** - Evacuate the area immediately. Do not use spark producing devices.
- **Poor or Closed Ventilation** - If smoke or burning odor is present, evacuate the area.
- **Elevator Challenge** - Push the emergency button or use the telephone in the elevator to contact Campus Security and Safety Department. Do not attempt to evacuate the elevator, unless instructed to do so by Emergency Response Team.
- **Plumbing/Flooding** - If personal safety allows, disconnect electrical devices and evacuate the area.
- **Electrical Problems**- Place Red Alert warning or sound and also quickly call the facility's management for prompt.

Food Service & its related dangers to disaster creation including food poisoning:

The Head and Supervisor of the University's Food Service Unit shall be responsible to ensure that:

- ✞ All gas tubes are properly checked for before, during and after cooking.
- ✞ Proper and adequate ventilation exist at all times
- ✞ Electrical cables running through their kitchens and restaurants are properly insulated.
- ✞ Food safety is hundred percent assured for staff and all members of the University community.

The University will also plan for the following three scenarios:

- ✞ Should an emergency render the Students residence hall uninhabitable, the affected residents will be moved into the unaffected building?
- ✞ Should an emergency create situation where no building on campus can be inhabited, the University vans and city buses will be used to transport residents to evacuation shelters until buildings become inhabitable. Blankets, pillows, and linen will be provided by volunteers from the faculty, staff and community. The Dean of Student Affairs and staff will develop a detailed plan to address each of the scenarios described above. The plan will also address cyclone notification and sheltering procedures.

Health and First Aid Services:

The Dean of Student Affairs, together with the Campus health facility and the Student Cadet Force and Red Cross Society shall be responsible for developing a health and first aid plan for emergency and disaster

situations. During a prolonged emergency or disaster situation, members of the Food Science faculty and the Campus Security and Safety Unit should be prepared to assist in health and first aid.

The health facility shall develop and maintain a list of first aid trained faculty staff members who can be called upon during a prolonged emergency. At a minimum, the Campus health facility will:

- Open the Student Health Emergency Center.
- Be prepared to treat all injuries of less than a critical nature that are the result of the existing emergency.
- All other shall be referred to a nearby government medical facility.

Emotional Trauma Response Services:

The Dean of Student Affairs, the Guidance and Counseling Unit in conjunction with the Director of Campus Sport and Recreation Programs shall be responsible for developing an emotional trauma plan for tragic and traumatic campus and community occurrences. In the event of a major tragedy affecting many individuals, the services of the Counseling Center may be improved by other professionals within the community on occasions like this. The campus Counselor will be involved in the coordination of these services. The Counseling Center will offer support to members of the campus community whenever such a major tragedy occurs. Support can take several forms, and may include, but not limited to, the following interventions:

✞ Individual support for those most affected.

✞ Group sessions for members who are impacted by a tragic event

✞ Programs open to the community to educate and discuss experiences.

✞ Continuous support for those whose negative reactions to the event are delayed or persistent. Special attention will be given to those who are already at risk for or diagnosed with a psychological disorder as traumatic events may aggravate their distress.

Persons who have vulnerability to depression, anxiety disorders, substance abuse, or other conditions that may be affected by the said tragic events, the Counseling Center Staff will educate the community about such risks and also inform the general community about the availability of counseling services for those individuals. The University Chaplain shall equally be required to provide support and assistance to the campus community in this regard.

Disaster Risks and Prevention

The establishment of DRM practices is important and shall allow the University to take strategic and operational measures to prevent or mitigate the effects a disasters beforehand. This portion of the Plan reviews the various threats that can lead to a disaster, i.e. all strategic and operational areas where our vulnerabilities are high, and put in effective recovery steps we to minimize our loses. The vulnerabilities covered here

could be both natural and human-created and the Plan is targeting the following areas.

- Fire Outbreak and Fire fighting
- Torrential rains an flood management
- Storms, Cyclone and High Winds Management solutions
- Earthquakes and landslides
- Cyber Crime
- Terrorist Actions Attacks and Sabotage
- Uncontrollable Student or Staff demonstrations
- Epidemics and pandemics
- Unplanned loss of key staff
- Sharp Political and regulatory changes
- etc.

Recovery from the Risk of Fire Outbreak and Poor Fire fighting

The threat of fire in any collegiate building, especially in the University's data center, is very real and poses the highest risk factor of all the causes of disaster mentioned here. This is because all the University buildings are filled with electrical devices and connections that could overheat or cause a fire.

The computer systems and the stored stationaries within the University's also pose a quick target for arson from anyone wishing to disrupt CCTU's operations. Wide area fires, such as those Kanneshie and Makola incidence could also be a possibility in dry seasons.

Preventive Measures Fire Outbreak

- **Fire Alarms:** All buildings, are to be equipped with a fire alarm system, with ceiling-mounted smoke detectors scattered widely throughout the building.
- **Fire Extinguishers:** Hand-held fire extinguishers are required in visible locations throughout all building. Personnel are to be trained in the use of fire extinguishers.
- **Building Construction:** The University Buildings shall be built primarily of non-combustible materials. The risk to fire can be reduced when new construction is done, or when office furnishings are purchased, to acquire flame resistant products.
- **Training and Documentation:** Detailed instructions for dealing with fire are present in Standard Operating Procedures documentation. Personnel are required to undergo training on proper actions to take in the event of a fire. Personnel are required to demonstrate proficiency in periodic, unscheduled fire drills.
- **Rescue Phones:** Rescue phones (wired) have been added to all floors and building to assist faculty, staff, and students during an emergency.

Recommendations:

1. Regular review of the procedures should be conducted to ensure that they are up to date.

2. Unannounced drills should be conducted by an impartial administrator and a written evaluation report should be produced for the department heads housed in these building.
3. Regular inspections of the fire prevention equipment are also mandated.
4. Fire extinguishers are periodically inspected as a standard Plan.

Recovery from the Risk of Flood Disaster

It is obvious majority of the University buildings are located on higher ground. The likelihood of a natural flood is low. However, a flood due to a water main break, sprinkler system malfunction, or roof leak is a strong concern. Flood waters penetrating rooms can cause a lot of damage. Not only could there be potential disruption of power caused by the water, flood waters can bring in mud and silt that can destroy sensitive electrical connections. Of course, the presence of water in a room with high voltage electrical equipment can pose a threat of electrical shock to personnel.

Preventive Measures

The facilities coordinator shall always be in direct contact with the all Directors and Deans on a continuing basis for any changes in water/sewer infrastructure within any of the University Buildings they occupy.

Recommendations

Periodic inspections of the mechanical/utility rooms must be conducted to detect water seepage; especially any time there is a heavy downpour. Operators should be trained in shutdown procedures and drills should be conducted on a regular basis. Contact phone numbers for building facility services are to be posted in the Front doors of each Office. Also, staff in the mechanical/utility rooms should be trained in responding to victims of electrical shock.

The Office of Information Technology should have large tarps or plastic sheeting available in the data center ready to cover sensitive electronic equipment in case the building incurs water damage. Protective coverings should also be deployed over backup storage units to prevent further water damage. Offsite backups should be deployed as standard practice. Operators should be trained how to properly cover the equipment.

Recovery from the Risk of High Winds

As the University is situated in high wind areas, damage due to high winds is a very real possibility. A high wind has the potential for causing the most destructive disaster we face.

High Winds Preventive Measures and Recommendations

Building construction makes a big difference in the ability of a structure to withstand the forces of high winds. Strong winds are often

accompanied by heavy rain, so a double threat of wind and water damage exists if the integrity of the roof is lost. Fortunately, the College of Public Health Building data center is located at the basement level and well protected from high winds.

Recommendations

All occupants of the University buildings on campus should know where the strong points of the building are and be directed to seek shelter in threatening weather.

Protective coverings should also be deployed over backup storage units to prevent water and wind damage. Offsite backups should be deployed as standard practice. Operators should be trained how to properly cover the equipment.

Recovery from the Risk of Earthquake

The threat of an earthquake in Central Region area is low, however management shall do all things possible not be ignored it since its effects can be catastrophic. Buildings in our area are not built to earthquake resistant standards like they are in quake-prone areas. So we could expect light to moderate damage from predicted quake. An earthquake has the potential for being the most disruptive for this disaster recovery plan. Restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do wide-scale building repairs.

Earthquake Preventive Measures and Recommendations

The preventative measures for an earthquake can be similar to those of a high winds and rainfall. Building construction makes all the difference in whether the facility will survive or not. Even if the building survives, earthquakes can interrupt power and other utilities for an extended period of time. Standby power generators could be purchased or leased to provide power while commercial utilities are restored.

Recommendations

The University Security Section should have large plastic sheeting available in the data center ready to cover sensitive electronic equipment in case the building is damaged. Protective coverings should also be deployed over backup storage units to prevent water and wind damage. Offsite backups should be deployed as standard practice. Operators should be trained how to properly cover the equipment.

Recovery from the Risk of Cyber-Crime

Cyber-crime is a significant threat to computer workstations and servers. With the increased availability of network accessible systems, the proliferation in cyber-attacks and unauthorized access exists. Cyber-crime usually does not affect hardware in a physically destructive manner. It may be more deceptive, and may often come from within. A disgruntled employee can build viruses or time bombs into applications and systems code. A well-intentioned employee can make coding errors

that affect data integrity (not considered a crime, of course, unless the employee deliberately sabotaged programs and data).

Cyber-Crime Preventive Measures and Recommendations

All systems should have security products installed to protect against unauthorized entry. All systems should be protected by passwords, especially those permitting updates to data. All users should be required to change their passwords on a regular basis. All security systems should log invalid attempts to access data, and security administrators should review these logs on a regular basis. All systems should be backed up on a periodic basis. Offsite backups should be deployed as standard practice. Physical security of the data storage for backups must be implemented. Standards should be established on the number of backup cycles to retain and the length of their retention.

Recommendations

Strictly enforce security policies and procedures. Regularly let users know the importance of keeping their passwords private and undisclosed. Let users know how to choose strong passwords or passphrases that are very difficult to compromise. Also as much as possible encourage all staff to use their Institutional emails for University transactions.

Steps should be taken to improve network security and intrusion detection. Shared network infrastructure, such as Ethernet and wireless

networking, are susceptible to sniffing activities, which unscrupulous users may use to capture passwords. Implement stronger security mechanisms over the network, such as one-time passwords, data encryption, and network monitoring.

Maintain good building physical security. Doors into the data center should be locked at all times. All visitors to the data center should receive prior authorization. Server and workstation operating system security, including the newest security patches, are important to maintaining a protected cyber environment.

Recovery from the Risk of Terrorist Action and Sabotage

Cape Coast Technical University as a public institution (University) can have the presence of Terrorist Action and Sabotage. Even though we as admit that Ghana as Country have not experience any such attacks in its public University. However incidence from our neighboring countries continues to put the Country and it public places to a high risk radar. In view of this it will be prudent for the University to put a recovery plan in this regards.

Preventive Measures and Recommendations to Terrorist Action and Sabotage

Good physical security is extremely important. However, terrorist actions can often occur regardless of in-building security, and they can be very destructive. A bomb placed next to an exterior wall of the data center will likely breach the wall and cause damage within the room.

Given the freedom that we enjoy within the Ghana, almost no one will accept the wide-scale planning, restrictions, and costs that would be necessary to protect the University as well as its surroundings from a bomb or other Terrorist Actions and Sabotage. However some commonsense measures can help.

Disaster Preparation

In order to facilitate recovery from a disaster which destroys all or part of the University or its data center, certain preparations have been made in advance. This document describes procedures for a quick and orderly restoration.

The topics for disaster preparation shall include:

- Disaster Recovery Planning
- Recovery Facility
- Replacement Equipment
- Backups

Disaster Recovery Planning

The preparation of this document very essential in the University wide risk management and recovery process. Thus to begin a process, a plan should be established. The overall plan should include responses to specific disasters as indicated above, while maintaining flexibility and adaptability.

Every Department or business unit within the University should develop a plan on how they will conduct business, both in the event of a disaster in their own building or a disaster within the entire university. The business units should develop procedures to function while the computers and networks are down. They should again plan how they will synchronize the data that is restored on the Central Administration with the current state of affairs.

Recovery Facility

If a central backup facility operated by the Central Administration is destroyed in a disaster, repairing or rebuilding of that facility may take an extended period of time. In the interim it will be necessary to restore computer and network services at an alternate site.

CCTU in this regards shall have a number of options for alternate sites, each having a varying degree of up-front costs.

Hot Site

This is probably the most expensive option for being prepared for a disaster, and is typically most appropriate for very large organizations. A separate computer facility, possibly even located in a different location, can be built, complete with computers and other facilities ready to cut in on a moment's notice in the event the primary facility goes offline. The two facilities must be joined by high speed communications lines so that

users at the primary campus can continue to access the computers from their offices and classrooms.

Disaster Recovery or Risk Assurance

As practiced elsewhere the University can adopt if possible, a number of companies provide disaster recovery services on a subscription basis. For an annual fee (or premium) you have the right to a variety of computer and other recovery services on extremely short notice in the event of a disaster. These services may reside at a centralized hot site or sites that the company operates, but it is necessary for you to pack up your backup tapes and physically relocate personnel to restore operations at the company's site. Some companies have mobile services which move the equipment to your site in specially prepared vans. These vans usually contain all of the necessary computer and networking gear already installed, with motor generators for power, ready to go into service almost immediately after arrival at your site.

Disaster Partnerships

As practiced elsewhere the University can adopt if possible, some organizations will team up with others in a partnership with reciprocal agreements to aid each other in the event of a disaster. These agreements can cover simple manpower sharing all the way up to full use of a computer facility. Often, however, since the assisting partner has to continue its day-to-day operations on its systems, the agreements are limited to providing access for a few key, critical applications that the

disabled partner must run to stay afloat while its facilities are restored. The primary drawback to these kinds of partnerships is that it takes continual vigilance on behalf of both parties to communicate the inevitable changes that occur in computer and network systems so that the critical applications can make the necessary upfront changes to remain operational.

Cold Site

A cold recovery site is an area physically separate from the primary site where space has been identified for use as the temporary home for the computer and network systems while the primary site is being repaired.

Replacement Equipment

This plan contains a complete inventory of the components of each of the computer and network systems and their software that must be restored after a disaster. The inevitable changes that occur in the systems over time require that the plan be periodically updated to reflect the most current configuration. Where possible, agreements have been made with vendors to supply replacements on an emergency basis. To avoid problems and delays in the recovery, every attempt should be made to replicate the current system configuration. However, there will likely be cases where components are not available or the delivery timeframe is unacceptably long. The University has the expertise and resources to work through these problems as they are recognized. Some changes may

be required to the procedures documented in the plan. Additionally, using different models of equipment or equipment from a different vendor may be suitable to expediting the recovery process. Leveraging virtual server technologies and cloud services will be considered.

Backups as a necessary evil

New hardware can be purchased. New buildings can be built. New employees can be hired. But the data that was stored on the old equipment cannot be bought at any price. It must be restored from a copy that was not affected by the disaster. There are a number of options available to us to help ensure that such a copy of your data survives a disaster at the primary facility.

Remote Dual Copy

This option calls for a disk subsystem located at a site away from the primary computer facility and fiber optic cabling coupling the remote disk to the disk subsystem at the primary site. Data written to disk or drive at the primary site are automatically transmitted to the remote site and written to disk or drive there as well. This guarantees that you have the most up-to-the-second updates for the databases at the primary site in case it is destroyed. You can simplify the recovery process by locating the remote disk subsystem at the disaster recovery site. This option is somewhat expensive, but not prohibitively so. It does not require that an entire computer system be built at a hot site, just the disk subsystem.

Off-Site Backup

This option calls for an offsite backup located at a site away from the primary computer facility and fiber optic cabling (the campus backbone network would be suitable) coupling the subsystem to the primary computer facility. Copies of operating system data, application and user programs, and databases can be transmitted to the remote tape subsystem where it is stored on magnetic tape (optical writable disk media can also be used, but may be more expensive).

While this option does not guarantee the up-to-the-second updates available with the remote dual copy disk option, it does provide means for conveniently taking backups and storing them off-site any time of the day or night. Another huge advantage is that backups can be made from mainframes, file servers, distributed (Linux-based) systems, and personal computers. Although such a system is expensive, it is not prohibitively so.

Cloud Deep Archive Storage

This option calls for the transportation of backup deep archive cloud storage. This type of backup is specific to disaster recovery. The drawback of the backup option is that it is expensive to run a restore and it tends to be a snapshot in time. The benefit is that you have a solid offsite backup of your data that is far away from Iowa City.

Stress Avoidance

Recovery from a disaster will be a very stressful time for all personnel involved. Each manager should be careful to monitor the working hours of his staff to avoid over-exertion and exhaustion that can occur under these conditions. A good approach is to divide your team members into shifts and rotate on a regular basis. This will keep team members fresh and also provide for needed time with family.

Establish the Recovery Control Center

The Recovery Control Center is the location from which the disaster recovery process is coordinated. The Recovery Manager should designate where the Recovery Control Center is to be established. If a location in the Office of Information Technology, is not suitable, the University can designated another location or center.

Activating the Disaster Recovery Plan

The Recovery Manager shall sets the plan into motion. Early steps to take are as follows:

1. The Recovery Manager should retrieve the Disaster Recovery Plan. Copies of the plan should be made and handed out at the first meeting of the Recovery Management Team.
2. The Recovery Manager is to appoint the remaining members of the Recovery Management Team. This should be done in consultation with surviving/remaining members of the University's Information

Technology staff and Facilities Management, for Administration approval.

3. The Recovery Manager is to call a meeting of the Recovery Management Team at the Recovery Control Center or a designated alternate site. The following agenda is suggested for this meeting:

1. Each member of the team is to review the status of their respective areas of responsibility.
2. After this review, the Recovery Manager makes the final decision about where to do the recovery.
3. The Recovery Manager briefly reviews the Disaster Recovery Plan with the team.
4. Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
5. Each member of the team is charged with fulfilling their respective role in the recovery and to begin work as scheduled in the Plan.
6. Each member of the team is to review the makeup of their respective recovery teams.
7. If a participant key to one of the recovery teams is unavailable, the Recovery Manager is to assist in locating others who have the skills and experience necessary, including locating outside help from other area computer centers or vendors.
8. The next meeting of the Recovery Management Team is scheduled. It is suggested that the team meet at least once each day for the first week of the recovery process.

4. The Recovery Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.
5. The Vice Chancellor is responsible for immediately clearing the Recovery Control Center room, for occupation by the Recovery Management Team. This includes the immediate relocation of any personnel occupying the room. Mobile communications will be important during the recovery process. This need can be satisfied through the use of mobile phones and/or two-way radios. University Facilities Management has two-way radio units that may be available upon request.
6. As soon as practical, a complete inventory of all salvageable equipment must be taken, along with estimates about when the equipment will be ready for use (in the case that repairs or refurbishment is required). This inventory list should be delivered to the Technical Coordinator and Administrative Coordinator who will use it to determine which items from the disaster recovery hardware and supplies lists must be procured to begin building the recovery systems.

6.5 Damage Assessment

This damage assessment is a preliminary one intended to establish the extent of damage to critical hardware and the facility that houses it. The

primary goal is to determine where the recovery should take place and what hardware must be ordered immediately.

Team members should be liberal in their estimate of the time required to repair or replace a damaged resource. Take into consideration cases where one repair cannot begin until another step is completed. Estimates of repair time should include ordering, shipping, installation, and testing time.

6.6 Emergency Procurement Procedures

The success or failure of this plan's ability to recover the university computer and network facilities hinges on our ability to purchase goods and services in a timely manner.

The Recovery Manager must have a sound financial plan (Budget) and procedures for aggressive recovery actions. Perhaps now is the time for a word of caution.

The Administrative Support Coordinator is responsible for all emergency procurement for the university's Office of Information Technology. All Disaster Recovery Team members must submit their requests to the Coordinator. The Coordinator will follow the regulations established for emergency procurement and will work with the Procurement Directorate for suppliers that has been appointed by the University to complete the acquisition.

The Administrative Support Coordinator is also responsible for tracking all acquisitions to ensure that financial records of the disaster recovery

process are maintained and that all acquisition procedures will pass audit review.

The Administrative Support Coordinator must also be aware of the University's insurance coverage to know what is and is not allowed under insurance policies. In the event an item to be purchased is disallowed by insurance coverage, or if expenses exceed the thresholds limits of the Vice Chancellor or the insurance coverage, the Coordinator must consult with the Recovery Manager and other responsible University personnel (such as the University's Council Chairman).

Maintaining the Plan

Having a disaster recovery plan is critical. However, the plan will rapidly become obsolete if a workable procedure for maintaining the plan is not also developed and implemented. This document provides information about the document itself, standards used in its construction, and maintenance procedures necessary to keep it up to date. Stress Avoidance

Recovery from a disaster will be a very stressful time for all personnel involved. Each manager should be careful to monitor the working hours of his staff to avoid over-exertion and exhaustion that can occur under these conditions. A good approach is to divide your team members into shifts and rotate on a regular basis. This will keep team members fresh and also provide for needed time with family.

GLOSSARY OF TERMS

Cold site: A cold site is an office or a data center that does not have any server installed. It has power, cooling, and space available if an organization's main work site or datacenter suffers a major outage.

Hot Site: Hot sites are essentially mirrors of your datacenter infrastructure. The backup site is populated with servers, cooling, power, and office space (if applicable). The most important feature offered from a hot site is that the production environment(s) are running concurrently with your main datacenter.

Cold Site: A cold site is essentially office or datacenter space without any server-related equipment installed. The cold site provides power, cooling, and/or office space which waits in the event of a significant outage to the main work site or datacenter. The cold site will require extensive support from engineering and IT personnel to get all necessary servers and equipment migrated and functional. Cold sites are the cheapest cost-recovery option for businesses to utilize.

Warm Site: A warm site is the middle ground of the two disaster recovery options. Warm sites offer office space/datacenter space and will have some pre-installed server hardware.

An offsite backup is a copy of a business' production system data stored in a geographically different location than the production system. Offsite backups include: Offsite server backup, where production data is backed up to an offsite server.

A cyber-attack refers to an action designed to target a computer or any element of a computerized information system to change, destroy, or steal data, as well as exploit or harm a network.

Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.

Performance bugs - programming errors that cause significant performance degradation - lead to poor user experience and low system throughput. Designing effective techniques to address performance bugs requires a deep understanding of how performance bugs are discovered, reported, and fixed.

Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Control activities - Control activities are the policies and procedures that help ensure management directives are carried out. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Corporate governance -*Is the structure of rules, practices, and processes used to direct and manage a company.*

Internal control - Is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance that the system or information is reliable, accurate and timely and also of compliance with applicable laws, regulations, contracts, policies and procedures.

***Key performance indicators* (*KPIs*) -** Are quantifiable measures that gauge a company's performance against a set of targets, objectives, or industry peers over a period of time.

What Are Key Performance Areas (KPAs) - Describe broad areas for which a department or organization or individual employee may be responsible.

Risk – Risk is anything that may happen that impacts the achievement of an organization's objectives. Risk is an event having a cause and a consequence that could be either positive or negative. Risk encompasses the following three dimensions: a. Hazard – Preventing an exposure from turning into a loss: b. Uncertainty – Coping with volatility and change; and c. Opportunity – Harnessing opportunities to one's advantage.

Risk exposure is the quantified potential loss from business activities currently underway or planned. The level of exposure is usually calculated by multiplying the probability of a risk incident occurring by the amount of its potential losses.

Risk Vs Exposure? The concept of risk can be simply captured in the equation: "**Risk = Hazard x Exposure**". For a hazardous object or situation to become a risk, there must be exposure. For example, a wild

and dangerous animal will always represent a hazard, but as long as it remains properly caged it will not represent a risk.

A disruptive event- Is an organizational-wide emergencies and disasters which are not covered by routine measures.

Risk Management – The process of identifying, assessing and developing management strategies to deal with risks at the enterprise level of the organization. It is measured in terms of probability and impact.

Risk Management Framework – A formalized process for managing risk on an explicit basis. The framework consists of a risk assessment, response and accountability for the risk and mitigation activities around it.

Risk culture - Is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose.

A risk action plan (RAP) - Is the course of action which an organization agrees upon to help them to address potential risks, reduce the likelihood of these risks occurring and to lessen the impact of these risks if they do occur.

A risk owner - Is an accountable point of contact for an enterprise risk at the senior leadership level, who coordinates efforts to mitigate and manage the risk with various individuals who own parts of the risk.

Contingency planning - Is a "what if" scenario management tool that involves all parts of an University and helps ensure timely and effective

aid to those who need it most before an emergency happens. A simple example of a contingency plan is to back up all website data before a website gets hacked.

Probability – A qualitative description of the likelihood and/or frequency of a risk occurring. **5. Impact –** The outcome of an event expressed in qualitative or quantitative terms (for example, financial or reputational) being a loss, injury, disadvantage or gain.

Risk Analysis – A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.

Risk Appetite – Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of objectives. It reflects that organization's risk management philosophy and, in turn, influences the organization's culture and operating style.

Inherent Risk – A raw risk that has no mitigation factors or treatments applied to it.