TAIF UNIVERSITY	INSTITUTIONAL POLICY AND PROCEDURE (IPP)	
Department: Deanship of Information Technology (ITD)	**Manual:** IT Policy and Procedure	**Section:** Database
TITLE/DESCRIPTION		**POLICY NUMBER**
Disaster Recovery and Business Continuity Planning		ITD-٠١٦

EFFECTIVE DATE	REVIEW DUE	REPLACES NUMBER	NO. OF PAGES
٢٥th Nov. ٢٠١٤		N/A	٠٤

APPROVED BY	APPLIES TO
Dean of Information Technology	Deanship of Information Technology

PURPOSE

This document designed to provide outlines in developing disaster recovery and business continuity plan. The Plan will serve as guidance in responding to catastrophic events involving university facilities and information technology services interruptions.

DEFINITION

I. **Disaster**: A serious disruption of the functioning of a community or a society causing widespread human. material, economic or environmental losses which exceed the ability of the altered community or society to cope using its own resources.

٢. **Disaster Recovery**: The ability to recover from the loss of a complete site. Whether due to natural disaster or malicious intent. Disaster recovery strategies include replication and backup/restore.

٣. **Disaster Recovery Plan**: The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan designed to assist in restoring the business process within the stated disaster recovery goals.

٤. **Business Continuity**: Preventative measures using redundant hardware. Software, data centers and other facilities to ensure that a business can continue operations during a natural or man-made disaster and if not. to restore business operation as quickly as possible when the calamity has passed.

RESPONSIBILITY

l. The Dean of IT is charged in ensuring that disaster recovery for critical information systems is developed. The dean is also responsible for monitoring. reviewing, and evaluating the compliance with this Plan.
٢. Department managers and other key officials are responsible for ensuring that offices and facilities under their control can operate despite information system service disruptions.

CROSS REFERENCES

ITD-٠٠٤ Data Backup and Recovery

POLICY

The University shall develop; periodically update, and regularly test its disaster recovery and business continuity plans to ensure the availability of the University's essential services in the event of an adverse impact to information systems due to a natural or man-made emergency or disaster event.

PROCEDURE

The following procedures outline the steps to be followed in the development and implementation of the disaster

recovery and business continuity plan:

١. Identify Mission Critical Functions

In the event of disaster, several functions will not be performed. Therefore. It is important to set priorities on their execution.

٢. Identify the Resources that Support Critical Functions

٢,١. Alter determining the critical functions; the resources that support the functions must also be identified. The amount of time and frequency of utilization must also be determined. This is an important factor since some resources are needed in daily basis while others are used only once a month. The objective of this procedures is to determine the impact if the resource is not available. To properly identify the mission critical functions and their impact, a Business Impact Assessment must be developed.

٢,٢. The Business Impact Assessment should include:

٢,٢,١ **Business Analysis** that identifies and describes critical functions, and high-level resources that support these functions. The Business Analysis will also describe the internal and external clients served by these functions. Through this analysis. We will able to determine the functional inter-dependencies and single points of failure.

٢,٢,٢ **Operational Impact Analysis** that identifies the organizational implications resulting from partial or total loss of access or information system facilities. The analysis will highlight which functions will be interrupted by the outage and the effects to both internal and external clients by such service interruptions.

٢,٢,٣ **Financial Analysis** that identifies the economic losses that could result from the outage. This analysis is optional but good to be included since the results will provide cost-justification for implementation and maintenance of specific recovery strategies.

٢,٣. To facilitate the better understanding of resources needs and their support to critical functions. A contingency planning team will be formed. The Team will include representatives from the functional/business groups, facilities management, and technology management. Specialized groups will also be assigned as needed to the Team. Members of these groups may include specialists in finance management, human resources, and information technology.

٣. Develops Recovery and Business Continuity Strategies:

٣,١. The purpose of this step is to plan how to recover needed resources and resume the operations after an outage. This step is critical in the development of Disaster Recovery and Business Continuity Plan because this will provide the specific guidelines by which the plan will be implemented.

٣,٢. The strategies development will include the following three (٣) important parts: emergency response, recovery, and resumption. The emergency response is the initial actions taken to protect lives and limit damage. Recovery refers to the steps to be taken to continue the support to critical functions. Resumption is the return to normal operations. The relationship between recovery and resumption is very important. The longer it takes to resume normal operations, the longer the Hospital will have to operate in the recovery mode.

٣,٣. In general, the strategy needs to be based on practical considerations such as feasibility and cost. Strategy development will be developed through the following steps:

٣,٣,١. Define Resource Requirements

Identify, through interaction with different departments' managers, the specific resources which are required for full and degraded operation of the functions performed by their respective department. Categorize these resources with similar recovery needs.

٣,٣,٢. Develop Recovery Alternatives

For each category, define the alternatives for recovery. In developing alternatives, several factors will be considered such as human resources, processing capability, automated applications and data, computer-based services, physical infrastructures, and documents.

٣,٣,٣. Recommend Recovery Strategy

From each alternative. select approach which will most effectively meet the Hospital‘s continuity and budget requirements Subsequently, present the recommended strategies to management for approval.

٤. Implementation

Implementing the strategies require much preparation. Below are the common implementation issues to be considered:

٤,١ Establishing procedures for backing up files and applications.

Backing up data and applications is a critical part of any disaster recovery plan. Backups are used to restore files alter a computer virus corrupted the data or after a fire raze the data center. The backups will be regularly tested to ensure that the data can be read from the disks and restored in the event that they are needed in an emergency.

٤,٢ Negotiate contracts and agreements.

The contingency strategies may require establishing contacts and agreements with recovery service vendors if it will meet or exceed the Hospital‘s needs both operational and financially.

٤,٣ Replacement of equipment.

If additional equipment is needed as the contingency strategies dictate, it must be maintained and periodically replaced when it is no longer dependable or obsolete to the University's information technology architecture.

٤,٤ Formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team.

٥. Documentation

٥,١ The plan will be documented and keep current as the personnel responsible for the implementation of the plan and other factors change.

٥,٢ The plan will be written in simple language and should clearly state the sequence of tasks to be performed in the event of a disaster so that someone with minimal knowledge can immediately begin to execute the plan.

٥,٣ The written plan will be kept in a secure environment including off-site locations if possible.

٥,٤ Each member of the contingency plan team will have copies of the Plan.

٦. Training

Concerned employees will be trained in their contingency-related duties. Refresher training may be needed and employees need to practice their skills. Training is important for effective employee response during disasters.

٧. Testing and Revising

٧,١ The Plan will be tested periodically to identify and correct any problems in the implementation. The Plan will become outdated as time passes and as the resources used to support the plan change. Test procedures may include the review of the plan, analyses, or disaster simulations.

٧,٢ The results of the test will be used to further improve the plan. If the University will not use this approach, flaws in the plan will remain undetected and not corrected.

FORMS

EQUIPMENT

REFERENCES

APPROVAL:

	Name	Signature	Date
Created by	**Hamed M. Hamed,** Sr. Database Administrator		Nov. ١٢th, ٢٠١٤
Reviewed by	**Musaed Al-Harbi,** Database Manager		Nov. ١٧th, ٢٠١٤
Reviewed by	**Anas Alqudsi,** Infrastructure Manager		Nov. ٠٥th, ٢٠١٧
Approved by	**Dr. Fawaz Alasseri** Dean of Information Technology		Apr. ٢٥th, ٢٠١٨