 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Business Continuity	Last Review date	10/05/2024
	Policy Number	ITC-09	Next Review date	10/03/2028
	Responsible Entity	Director if ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

Overview

This policy articulates requirements that assist management in defining a framework that outlines business continuity and disaster recovery plans, processes, procedures, testing, and reporting mechanisms that are to be in place and in effect to provide for continuity of the University of Sharjah's operations.

Scope

This policy is applicable to University of Sharjah's Faculty, employees and students including but not limited to, contractors, third party users, consultants, and temporary users at UOS who wish to access University of Sharjah's information assets. This policy also applies to all UOS information processing facilities.

Purpose

The main Purpose of this policy is to:

- Avoid the problems or any obstacles may stop the work and business operation.
- Ensure the achievement of overall business continuity objectives.

Abbreviations and Definitions

BCP: Business Continuity Plan

ITR: Information Technology Resources

DRP: Disaster Recovery Plan

COOP: Continuity of Operations Plans


RTO: Recovery Time Objective

RPO: Recovery Point Objective

BIA: Business Impact Analysis

Policy

- UoS shall ensure the achievement of overall business continuity objectives including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to information assets.
- UOS shall identify appropriate mechanisms to ensure that continuity plans are current and updated between annual tests and reviews accounting.
- UOS is required to develop, implement, test and maintain a Business Continuity Plan (BCP) for all Information Technology Resources (ITR) that deliver or support core Critical Business / academic Functions.


 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Business Continuity	Last Review date	10/05/2024
	Policy Number	ITC-09	Next Review date	10/03/2028
	Responsible Entity	Director if ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

- UOS shall develop; implement proper training and awareness plans to its employees that are responsible for supporting BCP.

Procedures

General

1. BCP is a plan that facilitates sustaining critical operations while recovering from a disruption. BCP's are required to include, at a minimum:
 - a. **Standard Incident Response:** An information system-focused set of procedures to be used when an event occurs that is not part of the standard operation of a service and may or does cause disruption to or a reduction in the quality of services and Customer productivity.
 - b. **Disaster Recovery Plan (DRP):** An information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure in the event of large scale disaster and/or other cataclysmic event.
 - c. **Continuity of Operations Plans (COOP):** An information system-focused plan invoked under a DRP when access to the primary facility infrastructure is prevented for an extended period, requiring operations to be restored from an alternate site after an emergency.
2. UOS shall conduct risk assessments to identify, estimate, and prioritize risks to enterprise operations.
3. Conduct business impact analyses to identify all critical functions of the university, which needs to be reviewed yearly.
4. UOS shall define information, which includes the details necessary to effectively respond, manage, and recover from an incident.
5. UOS is required, at a minimum, to include the following documentation in their BCP and its supporting components:
 - a. Scope / Objectives
 - b. Risk Evaluation and Required Security Controls
 - c. Business Impact Analysis
 - d. Communications Procedures
 - e. BCP Organization Structure
6. All third party vendors shall sign and accept their obligations to meet University's business continuity requirements.
7. UOS shall securely store copies of plans and supporting materials in a remote location
8. UOS shall document, implement and test the plans annually. Testing also include appropriate security provisions to minimize the impact to systems or processes from the effects of major failures of IT Resources or disasters.
9. UOS shall identify appropriate mechanisms to ensure that continuity plans are current and updated

 جامعة الشارقة UNIVERSITY OF SHARJAH	Policy Main Title	Information Technology Center	Effective Date	30/05/2021
	Policy Subject	Business Continuity	Last Review date	10/05/2024
	Policy Number	ITC-09	Next Review date	10/03/2028
	Responsible Entity	Director if ITC	Approved By	Vice Chancellor for Financial and Administrative Affairs

between annual tests and reviews accounting for:

- a. Change management implications
- b. New/Major upgrades of system implementations
- c. New policy adoption
- d. New contract implementations
- e. New threat/risk identification
- f. Staff/resource/responsibility changes

Roles and Responsibilities

Recovery Manager & Deputy Recovery Manager

1. Approves the final Business Continuity Plan.
2. Ensures that the Continuity Plan is maintained and updated.
3. Ensures that adequate training is conducted for all concerned.
4. Authorizes periodic Plan testing and reviews results.
5. Declares that a disaster has occurred and the activation of plan.
6. Determines resources to be allocated at the time of a Disaster.
7. Authorizes travel, housing arrangements and other expenditures for team members.
8. Manages and monitors the overall recovery process.
9. Advises senior management on the status of the disaster recovery efforts.

Legal, Marketing & Communications In-charge

1. Prepare emergency communication messages to customers, vendors and media.
2. Ensure all recovery procedures are compliant to legal and regulatory requirements.
3. Ensure legal compliance for existing policies and procedures.

IT & Information Security Recovery Lead

1. Lead the recovery for all IT systems.
2. Ensure compliance with Information Security Policies during disaster as much as possible.
3. Ensure Backup and restoration procedures are tested and documented.
4. Ensure hardware and software inventories are maintained.
5. Ensure that Recovery of IT systems meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) figures identified in the Business Impact Analysis (BIA).
6. Plan and coordinate testing of IT systems as part of Continuity Plan Testing.

Reference

SI No	Standard Name	Control Reference
1	ISO 27001:2013	A.6.1, A.6.2, A.6.3, A6.4, A6.5