Arab Open University
Business Continuity Policy

Policy Title:	Arab Open University Business Continuity Policy
Version Number:	4
Executive Owner:	Chief Information Officer
Approving Authority	University Council # 75, March 2022
Policy Review:	IT Policy Review Committee 2021 CIO Council
Policy Implementation:	AOU Campuses/ Branches
Policy Monitoring and Compliance:	IT Steering Committee IT Manager Quality Assurance and Accreditation Department
Next Review Date	March 2027

Note: *A policy can be reviewed before the designated review date should there be a need to.*

Contents

Introduction

A business continuity policy is a guideline to prepare a continuity plan including collection of procedures, information and processes, which are developed, compiled and maintained in readiness for use in the event of an emergency or disaster. A single downtime might mean a disaster to the business. Therefore, the traditional Recovery Plan, which focuses on restoring data and operation, might not be adequate. A more comprehensive and rigorous Business Continuity Policy (BCP) is needed to achieve business continuity where critical systems are continuously available. AOU is committed to providing its services to all stakeholders (students, staff, and the wider community) with minimum disruption. This BCP supports AOU's business operations continuity, mitigation of risk, and prescribes business processes recovery.

Objective

A well-developed Business Continuity policy helps AOU minimize the disruption of its business due to disasters. This enables AOU to sustain its business, provides its clients with better assurance of AOU's capabilities of responding to emergencies and protects its image and reputation in the market. This policy forms a part of AOU's risk management framework and aims at minimizing the adverse effects of business interruption due to emergencies and providing the appropriate response for mitigation of related risks. Effective compliance with this policy safeguards AOU's reputation and enhances its public image by ensuring that its mission-critical operations such as tutoring, research, and community services are running without interruption.

Responsibility

The Business continuity management team is responsible for developing & implementing this policy and tested periodically. The BCM team consists of the following members.

1) President
2) Vice President for Planning and Development

3) Vice President for Academic Affairs and Scientific Research
4) Chief Information Officer
5) Director at the Campus/Branch level
6) Head of Registration
7) Head of Information Technology
8) Head of Human Resources
9) Head of Procurements
10) Head of Finance
11) Head of Operations and Maintenance

Scope

The AOU IT department seeks to achieve the status of the "Best" IT Infrastructure and Services – to provide relevant, lifelong education of exceptional quality IT solutions available to everyone, no matter whom or where they are.

The BCP applies to AOU community members and all AOU premises including branches.

Policy Statement

The responsibility for implementing the AOU BCP lies with the Business Continuity Management Team (BCMT) which is responsible for identifying the possible threats/risks/vulnerabilities, analysis, and assessment of impact on AOU services and formulating the necessary actions for mitigation and recovery. Implementation of the BCP includes detailed procedures and support agreements with external bodies and other university branches to ensure prompt service recovery and business continuity. Monitoring effective compliance this policy is the responsibility of the (BCMT). An annual review must be conducted in addition to workshops for training and evaluation of the AOU Business Continuity plans.

Key Components of an Effective Business Continuity Plan

1) Chain of Command
1) Risk Assessment & Response
2) Core Business Systems
3) Business Continuity Management Team
4) Key Contacts
5) Staff Contact Details
6) Recording Incidents
7) Training
8) Review & Test Your Business Continuity Plan
9) Critical Document Names & Storage

Principales

The BCMT is committed to:

1) Mitigate business interruption risks, recover and continue the mission-critical operation as promptly as possible.
2) Ensure the safety and health of its staff.
3) Safeguard AOU assets.

Disaster Recovery Plans

All AOU branches are required to have disaster recovery and business continuity plans to ensure continuity of mission-critical operations and services.

Policy Compliance Certification and Support

The BCPT follows up implementation and compliance by AOU branches and ensures that heir BCP plans include the appropriate procedures, staffing, tools, and AOU requirements necessary for meeting deliverable requirements. All BCP alternative sites documents should follow the format prescribed in AOU approved templates.

BCPMT supports all branches in the development of their respective BCP and relevant processes.

AOU strives to maintain and continue to provide its services to all stakeholders that requires the commitment of each employee, department, and business partner in support of protecting AOU assets in pursuit of its strategic objectives, mission, and vision.

Related Policies

- AOU Strategic Plan
- AOU IT Disaster Recovery Plan
- AOU Risk Register
- AOU Data Protection Policy
- AOU Network Security Policy
- Related SLAs with vendors
- AOU Business Continuity Plans