Division: **Finance and Administration**
Department/Unit: **Information Technology**

Policy Title:	**IT Business Continuity Management System**				
Policy Number:	FA.IT.8.0-PP	**Version:**	1.0	**Effective Date:**	Spring AY 24-25
Owner:	Information Technology Department	**Participants:**	ISO Consultant		
Date recommended by the Divisional Council/Committee:	00/00/0000	**Institutional Council/Committee Approval:**	NA		
AY due for Review: *(After 5 years)* **If not within the review cycle, indicate the reason:**	AY 29-30	**Reviewed:** NA	**With modification:**		-
			With no modification:		-

I. Policy Statement:

Dar AlHekma University understands the critical need to safeguard its assets, operations and services to protect the interests of its stakeholders. In support of national initiatives aimed at automating and enhancing service accessibility for students, faculty, and staff, the University is committed to establishing a comprehensive plan for the continuity and recovery of its electronic services (e-services) in the event of a disaster. The University is also dedicated to facilitating recovery efforts at alternative facilities when necessary.

II. Purpose:

This policy establishes the objectives, scope and key principles for business continuity management at Dar AlHekma University.

III. Scope:

A. FA Division:

1) Information Technology Department.

2) Suppliers and outsourcing partners involved in BCMS.

IV. Policy Provision:

A. The Information Technology Department at Dar AlHekma University plays a crucial role in delivering high-quality IT services to stakeholders. The department is dedicated to ensuring uninterrupted service and protecting stakeholder interests, both of which are key to the department's long-term sustainability.

B. The IT Business Continuity Management System (BCMS) covers critical units, functions, and processes that require a recovery plan. The IT Department utilizes both proactive and reactive strategies to minimize the impact of major incidents, including:

1) Implementing a risk assessment and impact analysis plan aligned with the ISO 22301 requirements

2) Developing recovery plans to mitigate significant risks.

3) Integrating business continuity and disaster recovery (DR) planning into all operational requirements.

4) Using third-party service providers to maintain appropriate and tested recovery strategies if necessary.

5) Designing critical alternatives for continuous operation during system failures.

6) Preparing, testing and auditing plans, as well as conducting drills to ensure readiness if needed.

7) Improving the effectiveness of the business continuity management system continuously.

C. The policy shall be communicated to the Information Technology Department personnel to ensure strict compliance .

D. Each unit in the IT department is responsible for maintaining its business continuity management preparedness at all times. E. Head of the Finance and Administration Division ensures business resilience by committing to:

1) Providing the necessary resources to uphold the IT business continuity management system.

2) Ensuring thorough risk assessments and business impact analyses tailored to the operations, enabling the IT Department to manage risks effectively and implement control measures.

3) Ensuring the development and regular review of the IT Business Continuity Plan to maintain the continuity and safety of the team, facilities, and operations.

4) Ensuring that business continuity plans are effectively communicated throughout the IT Department.

5) Ensuring the IT Department complies with customer specifications, international standards, and local regulatory and legal requirements.

6) Ensuring the IT Department is knowledgeable about the Business Continuity Management System and is prepared to respond in the event of a disruption.

7) Identifying the Business Continuity Team, clearly defining their roles, and providing them with appropriate training.

8) Considering the sustainability requirements.

9) Reviewing IT BCMS policy, objectives, plans, and impact analyses on a predefined cycle.

V. Procedure(s) that apply:

NA

VI. Flowchart:

NA

VII. Applicable Form(s):

NA

VIII. Definition(s):

Word/Term	Definition
BCMS	Business Continuity Management Systems

IX. Related Policy(ies):

1. PO.4.0. PP - Risk Management
2. PO.QA.9.0. PP - Records Retention
3. FA.2.0-PP - E-Document Control
4. FA.HR.8.0-PP - Employee Training and Development
5. FA.HR.42.0-PP- Leadership Practice

X. Related Procedure(s):

1. FA.IT.8.1.PR - Context of organization procedure
2. FA.IT.8.2.PR - Control of document procedure
3. FA.IT.8.3.PR - Internal Audit procedure
4. FA.IT.8.4.PR - Management review procedure
5. FA.IT.8.5.PR - Corrective action and Nonconformity procedure
6. FA.IT.8.6.PR - Communication participation procedure
7. FA.IT.8.7.PR - Legal compliance procedure
8. FA.IT.8.8.PR - Business Continuity Procedure
9. FA.IT.8.9.PR - Monitoring and measurement procedure
10. FA.IT.8.10.PR - Change management procedure

XI. Reference(s):

ISO 22301 standard, clauses 4.1, 4.3, 5.3, 6.2 and 9.1.1

XII. Policy History:

1. Version 1.0: 30/10/2024 (Policy Created)

XIII. Contact(s):

Department:	**Information Technology Department**
Division :	**Finance and Administration**
Telephone :	+ 966 12 630-3333 Ext:
Email :	sdp@dah.edu.sa

XIV. Approvals:

Reviewed by: (signed)	**Ms. Salwa Abdulraqib**	**Recommended by: (signed)**	**Ms. Rasha Almalik**	**Approved by: (signed)**	**Ms. Huda Abdulraqib**
Position:	**Chair of QASP Council**	**Position:**	**Chair of ITQAC**	**Position:**	**Chair of FAQAC**