جامعة دار الحكمة
DAR AL-HEKMA UNIVERSITY

IT Business Continuity Strategy

Academic Year 2024-2025

Finance and Administration Division

Table Of Contents

I. Introduction

Dar Al-Hekma University recognizes the critical importance of safeguarding its digital infrastructure, operations, and services to ensure the continued success and satisfaction of its stakeholders. As part of the national vision to digitize and streamline services across higher education institutions, the University is committed to implementing robust strategies for disaster recovery and the continuity of electronic services (e-services).

In line with this commitment, Dar Al-Hekma University aims to maintain a comprehensive and effective plan that supports the swift recovery of services. This plan reflects the University's dedication to ethical standards, strategic alignment, and operational resilience—ensuring uninterrupted delivery of high-quality services to students, faculty, and staff.

The Information Technology Department at Dar Al-Hekma University was established to lead the management, development, and security of the university’s digital environment. It plays a pivotal role in advancing the university’s mission through technology-driven solutions that support academic excellence, research, and administrative efficiency.

II. Vision

A university that takes the lead in education, development, and creativity to positively impact the society.

III. Mission

Graduating leaders and entrepreneurs who embody the values of the university by providing an educational environment that encourages development, creativity, scientific research, and community service.

IV. Values

A. Quest for Excellence:

Dar Al-Hekma strives to promote and pursue excellence in all forms and ways, be it through curricular or extra-curricular pursuits; personal or institutional; individual or team effort

B. Vision for the Future:

Dar Al-Hekma, as a visionary community, values creative and innovative learning that preserves, protects and advances the human, social and physical environment, while building the knowledge base to assure a sustainable future for all

C. Creativity and Innovation:

Dar Al-Hekma embraces new ideas and encourages innovation with an entrepreneurial spirit

D. Appreciation for Knowledge:

Dar Al-Hekma values knowledge attained through diverse means of teaching and learning methodology and honors the sources of knowledge

E. Service to Community:

Dar Al-Hekma values its obligations to the larger community and ensures through the design and delivery of all its academic programs and services that the community is well served

V. IT Mission:

To enhance the educational experience and operational efficiency by integrating cutting-edge technology, fostering digital literacy, and promoting a culture of continuous innovation and improvement.

VI. Scope:

All critical business processes within the Information Technology Department, including infrastructure, assets, and personnel, ensure the continuity and resilience of the University's digital infrastructure.

A. Governance structure

The governance of the **Business Continuity Management System (BCMS)** at IT Department at Dar Al-Hekma University ensures senior management involvement and a structured approach across the institution. The roles and responsibilities include:

1. ***Executive Leadership (Senior Management)***

To Oversee and endorse the BCMS, ensuring it aligns with the IT Strategic Plan and the University's strategic objectives.

2. ***BCM Manager***

To Oversee day-to-day operations of the BCMS. Develop, update, and maintain BCPs and DRPs, conduct risk assessments, and coordinate responses during disruptions. Present the strategy and annual plan progress in the "ITQAC", "FQAC" and "UPC".

3. ***Unit Managers (IT Department)***

To Ensure IT service continuity within their areas. Ensure resource availability for recovery, support the BCM Manager, and maintain readiness for disruption responses.

4. ***Incident response and Disaster Recovery Team***

Activated during disruptions to coordinate Incident response and disaster recovery. Make key decisions, ensure effective communication, and oversee recovery strategy implementation.

5. ***All Staff and Personnel***

All employees must understand and follow the BCMS. Follow recovery procedures and report incidents.

6. ***Policies and Procedures***

An available policy and several procedures are available to govern the processes of the Business Continuity Management System.

VII. Business Continuity Strategy

A. Prioritize and Categorize

Developing business continuity strategies involves deriving recovery methods from the **Business Impact Analysis (BIA)** and **Risk Assessment (RA)** activities. The goal is to create a continuity plan that aligns with the needs of the business, addressing risks that could disrupt the continuity of critical operations in the **IT Department** at Dar Al-Hekma University. These strategies also ensure that investments in the **Business Continuity Management (BCM)** system are well-justified.

The **IT Department** has developed a comprehensive business continuity strategy that focuses on:

1. Protecting prioritized business processes and their supporting activities.
2. Stabilizing, continuing, resuming, and recovering prioritized processes and dependencies.

3. Mitigating, responding to, and managing the impacts of disruptions.

The **BCM Manager** evaluates the business continuity capabilities of suppliers to ensure reliable recovery methods in case of disruptions.

The BCMS team at IT Department identifies and manages both internal and external dependencies critical to IT processes. This includes understanding how these dependencies impact continuity and ensuring that recovery strategies are aligned with these interconnections.

B. Key Assumptions & Considerations

1. General Assumptions:

a. This strategy covers continuity for prioritized IT services at **Dar Al-Hekma University**, with **RTOs** ranging from 0 hours to 1 day, as identified in the **BIA** report.

b. If any disruption exceeds the RTO threshold (1 day), the IT department will take additional actions to ensure business resilience, including setting up full-functional recovery facilities if required.

2. HR Requirements:

a. It is assumed that the minimum number of personnel required for recovery activities are available.

b. Each unit manager within the IT Department assists the **BCM Manager** in the recovery and resumption of services.

c. Unit Managers, with support from BC Planner, **IT** and **Facilities**, will ensure the availability of personnel, necessary equipment, and vital records.

3. Technology Requirements:

a. The **IT Disaster Recovery (DR)** plan will be integrated with the broader **BCM** plan.

b. As of now, the IT department operates an off-site backup. However, a separate IT DR site for the critical operations has been planned and started.

4. Vital Records:

a. Vital records for the recovery of each prioritized IT service are documented in the Business Continuity Plans for each unit within the IT Department.

C. Protection & Mitigation Roadmap

To address identified risks, **Dar Al-Hekma University IT** should implement proactive measures to:

1. **Reduce** the likelihood of disruption.

2. **Shorten** the disruption period.
3. **Limit** the impact on key IT services.

Outage Scenarios	Selected Strategy Options	Recommended Protection and Mitigation Actions	Recommended Initiation Timeframe
General	N/A	- Raise awareness of disaster scenarios and threats for IT staff and stakeholders. - Regularly update key documents such as business continuity plans and recovery procedures. - Periodically test recovery plans and procedures. - Activate the Incident Response plan when needed.	Immediate action required: ASAP
Unavailability of the Work Facility	Staff can work from home.	- Implement safety and emergency protocols for university facilities. - Establish an alternate DR, and VPN Access.	Immediate action required: ASAP
Unavailability of Employees	Cross-train resources and distribute staff across multiple responsibilities	- Identify key human resources and backups in each IT unit. - Provide training across critical teams.	Immediate action required: ASAP
IT Services Outage	Develop DR site for SIS and IT data center.	-Develop redundancy in critical systems and infrastructure. - Migrate to cloud SaaS, and IaaS	Immediate action required: ASAP
Operational Disruption	Identify workarounds to avoid bottlenecks in impacted processes.	- Revise the design of impacted processes and implement simplified workflows for emergencies.	Urgent action required: Within 5 working days

D. Testing Exercising and validation:

IT conducts thorough **testing and exercising** of its recovery plans. This ensures that the BCMS remains effective and ready to be activated in the event of disruption.

1. **Regular Testing and exercising**: The IT department, along with key stakeholders, performs scheduled testing of the Business Continuity Plans (BCPs). These tests simulate different disaster scenarios testing both the communication protocols and the recovery procedures to evaluate response times, resource availability, and overall plan effectiveness.
2. **Plan Validation**: After each exercise, a comprehensive review is conducted to identify gaps, inefficiencies, or areas for improvement. Any issues are addressed, and recovery plans are updated accordingly. The results of these tests and exercises are documented and used to continually enhance the BCMS.

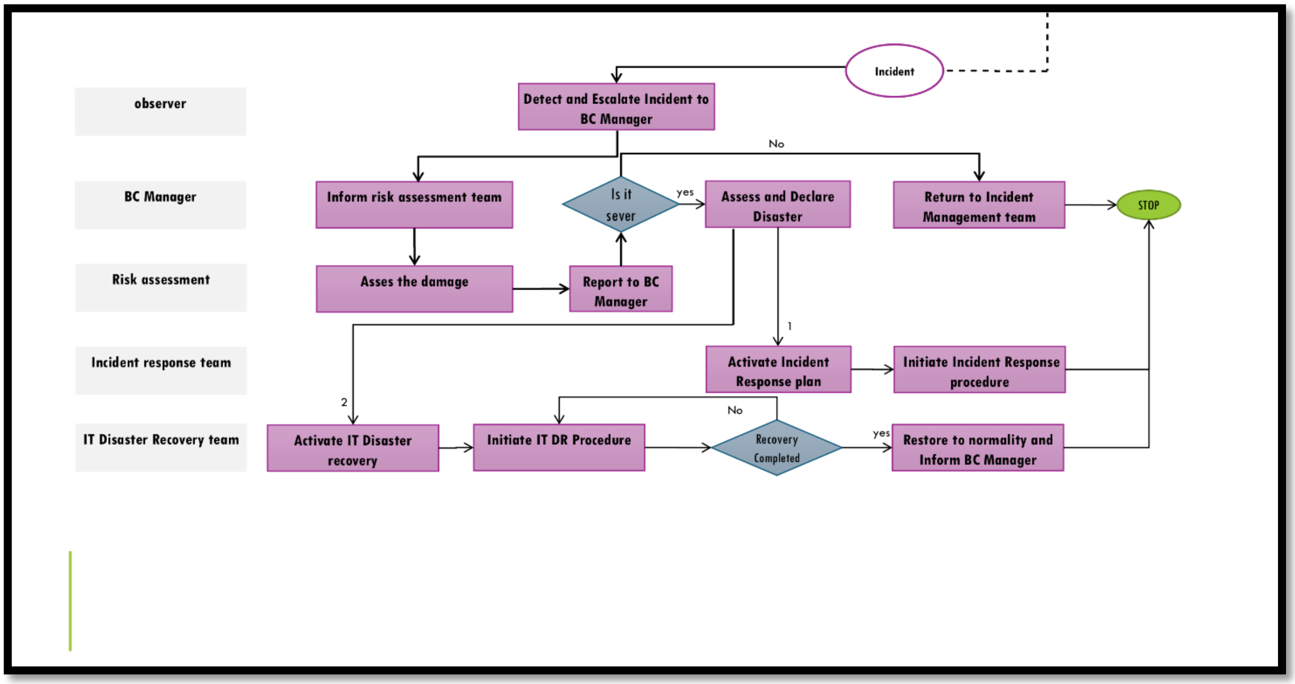
E. Determination & Selection

The recovery strategy selection is based on the nature of disruption and its potential impact on the IT services at **Dar Al-Hekma University**. The following table outlines the potential scenarios and the corresponding recovery strategies:

Description	Facility Data Center	People Recovery Strategy
Business as usual	N/A	N/A
Primary facility unavailable	SaaS and DR Systems	Remote working
Primary IT unavailable	Restore from Off-site backup, SaaS and DR Systems	N/A

F. Process Flow

In the event of a disruption to IT services, a series of activities will be carried out to report the incident and recover services. The high-level process flow diagram will guide the recovery activities, which are detailed in subsequent sections. Throughout the process, **crisis communication** is vital to ensure timely dissemination of information to all stakeholders and protect the university's reputation.


Incident
observer
Detect and Escalate Incident to BC Manager
No
BC Manager
Inform risk assessment team
Is it sever
yes
Assess and Declare Disaster
Return to Incident Management team
STOP
Risk assessment
Asses the damage
Report to BC Manager
1
Incident response team
Activate Incident Response plan
Initiate Incident Response procedure
2
No
IT Disaster Recovery team
Activate IT Disaster recovery
Initiate IT DR Procedure
Recovery Completed
yes
Restore to normality and Inform BC Manager

D1. High-level process flow diagram

G. Detect, Assess, and Declare Disaster

Disasters are significant disruptions that cause critical IT services to be unavailable for an extended period, impacting university operations. The most common sources for identifying a disaster include:

1. **IT Operations and Technical Support**
2. **Information Security** (major breaches or attacks)
3. **Network and Internet Services**
4. **Building Management/Physical Security** (e.g., fire, flood, bomb threats)
5. **External Observers** (e.g., staff, emergency services)

In the case of an incident, it can be reported through the following channels:

1. Directly to the **BCM Manager**.
2. Through the **Observer's Reporting Manager** or **Supervisor**.
3. **Administration**, or HR
4. Incident tracker System, Change management form
5. **IT Helpdesk**.

Once the incident is reported, the **BCM Team Leader** will assess the severity and decide if a disaster declaration is needed. If a disaster is declared, the continuity and recovery procedures will be activated to restore normal operations as quickly as possible.

VIII. Business Continuity Plans

The IT Department has developed and documented comprehensive **Business Continuity Plans (BCPs)** designed to effectively respond to and manage any disruptions caused by incidents or crisis. This plan outlines recovery strategies to restore IT services within a predetermined timeframe, ensuring minimal impact on the university's operations.

The **Business Continuity Plan** encompasses the following interrelated phases:

1. **Incident Response Plan:** It defines immediate actions to contain and manage the incident, focusing on stabilizing IT systems and minimizing further damage. It ensures swift on-site responses to prevent escalation and protect critical IT infrastructure.
2. **Disaster Recovery Plan:** It focuses on restoring IT services and infrastructure after a major disruption, ensuring recovery of critical functions within established recovery time objectives (RTOs). It includes backup systems, data restoration, and access to alternate IT sites.

All detailed Business Continuity Plans—including the IT Incident Response Plan and the IT Disaster Recovery Plan—are documented in full in the **appendices** of this strategy. These appendices contain comprehensive roles, responsibilities, response workflows, and recovery procedures to ensure effective operational continuity and alignment with ISO 22301 standards.

IX. Key Terms and Definitions

Term	Definition
Senior Management	Refers to the University Planning Committee (UPC)
Top Management	Refers to Finance and Administration Quality Assurance (FQAC)
BCMS Manager	The head of IT department and IT Quality Assurance Committee
BCMS	Business Continuity Management System
RTO	Recovery Time Objective
DR Site	Disaster Recovery location

Recommended by: **(signed)**	**Ms. Rasha Almalik**	**Approved by:** **(signed)**	**Ms. Huda Abdulraqib**
Position:	**Director – Information Technology Chair of ITQAC**	**Position:**	**Executive Director – Finance and Administration - Chair of FAQAC**

- This document is the property of Dar Al-Hekma University (Jeddah)
- The following instructions must be followed:
  - Any document that is not printed on paper marked as document control shall not be considered
  - Maintains the original certified copy with live signatures with the Director of the Quality Assurance Department
  - It is not permissible to write, cross out or modify certified copies
  - It is not permissible to modify, add or reissue except through the Director of the Quality Assurance Department

Appendix

A. IT Incident Response plan

1. Purpose and Objectives:

a. Purpose:

The purpose of this plan is to enable the IT Department to effectively respond to and manage the impact of an emergency or crisis, ensuring a swift and efficient recovery. It is designed to provide a structured approach for resuming normal business operations with minimal disruption.

b. Objectives:

- **Identify and prioritize critical functions and activities of the IT Department at DAHU** to ensure business continuity during and after a crisis.
- **Assess and mitigate risks** to the IT Department at DAHU, focusing on potential threats that may disrupt critical operations.
- **Develop a clear, prioritized, and time-bound response plan** for managing emergencies, ensuring a swift recovery of essential IT services.
- **Define key roles, responsibilities, and communication channels** to ensure effective coordination and response during an emergency or crisis.

2. Critical Function Checklist

Priority	Critical function	Timeframe
1	**Availability of Students Information System (SIS)**	6 hrs.
2	**Internet and Network Infrastructure**	7 hrs.
3	**Availability of Blackboard**	12 hrs.
4	**Availability of the website**	8 hrs.
5	**File Server**	6 hrs.

This list may be used as a checklist to ensure that critical tasks are completed on time and according to a pre-agreed priority schedule. It may also be used to provide a hand-over document between different shifts in the recovery process.

3. Command and Control

The decision to activate this plan will be made by the **Executive Leadership**, **IT Quality Assurance Committee**, or designated **IT Department Director**, who will be responsible for overseeing and directing the overall response. These leaders will also make critical decisions regarding the IT Department's priorities and actions during the crisis, ensuring that necessary resources are allocated, and the University's objectives are effectively supported throughout the disruption. (Refer to the attached IRP contact list for further details.)

4. Critical Function Analysis and Recovery Process

<table>
<tr><td><b>Priority:</b></td><td><b>1</b></td><td><b>Critical function:</b></td><td><b>Availability of Students Information System (SIS)</b></td></tr>
<tr><td colspan="3">Responsibility:
<i>(Role responsible for leading on this activity, plus deputies)</i></td><td>Senior System Administrator
Database Administrator
Network manager
Security administrator</td></tr>
<tr><td colspan="3">Potential impact on the University
if interrupted:</td><td>1. <b>Disruption to Student and Administrative Services</b>
• Enrollment & Registration delays
• Inaccessibility to Grades & Transcripts
• Financial Aid & Billing issues
2. <b>Student Satisfaction & Reputation</b>
• Negative Impact on Student Experience
• Potential decline in Retention
3. <b>Security Risks</b>
• Increased Risk of Data Breaches</td></tr>
<tr><td colspan="3">Likelihood of interruption to university:</td><td>Possible</td></tr>
<tr><td colspan="3">Recovery timeframe:
<i>(How quickly must this function be recovered to avoid lasting damage)</i></td><td>6 hrs
(The function must be restored within 8 hours to avoid significant operational, financial, and reputational damage)</td></tr>
<tr><td colspan="4"><b>Resources required for recovery:</b></td></tr>
<tr><td colspan="3"><i>Staff</i>
<i>(Numbers, skills, knowledge, alternative sources)</i></td><td>1. 4-5 IT specialists (System Administrators, Database Administrators, and Network Specialists)
2. Skills: Expertise in SIS (Banner), Database Recovery, Network Management, Cloud Services, Security tracking and logging.
3. Knowledge: System Configuration, Backup/Restore Procedures, Disaster</td></tr>
</table>

	Recovery Processes. 4. Alternative sources: In the event of unavailability, external consultants specializing in Banner/SIS systems may be required, SLA with Taqniyat (Banner Partner), Third party for oracle cloud support
Data / systems *(Backup and recovery processes, staff and equipment required)*	1. **Backup and recovery processes**: Regular backups of SIS data stored on cloud-based servers (oracle). 2. **Staff and equipment required**: Cloud Restoration, Cloud DR.
Premises *(Potential relocation or work-from-home options)*	1. **Shifting to Banner DR – in Riyadh**: In case of a regional disruption (such as a power outage or natural disaster in Jeddah), operations will be shifted to a disaster recovery site in Riyadh. 2. **Work-from-home options** for staff in case of local disruptions affecting physical on-site infrastructure.
Communications *(Methods of contacting staff, suppliers, customers, etc)*	1. **Internal communication**: Email and Mobile (SMS, WhatsApp) 2. **External communication**: Contact suppliers/vendors through email and phone. In case of significant disruption, communicate with students via university social media and website updates. Refer to **Section 6: Contact Lists** for full contact information.
Equipment *(Key equipment recovery or replacement processes; alternative sources; mutual aid)*	**Key equipment recovery or replacement processes**: • Backup of off-site tapes for rapid recovery. (for historical data from the legacy system) • **Backup Instances & DR**: Ensure **cloud backups** and **failover** setups in Oracle's **multi-region** infrastructure. • **Monitoring & Alerts**: Use **Oracle Cloud monitoring** for real-time health checks and issue alerts. • **Support**: Utilize **Oracle's 24/7 third party support** for rapid recovery.
Supplies *(Processes to replace stock and key supplies required; provision in emergency pack)*	• Cloud Backup policy

Priority:	**2**	**Critical function:**	**Internet and Network Infrastructure**
Responsibility: *(Role responsible for leading on this activity, plus deputies)*			1. **Network Manager** 2. **Security Administrator** 3. **Deputies**:

	a. **Network Support Team** (for troubleshooting and recovery) b. **Operations Team** (for general support and coordination)
Potential impact on university if interrupted:	1. **Operational Disruption**: • Core business functions are disrupted, impacting operations. • Delays in projects and tasks due to system unavailability. 2. **Communication Breakdown**: • Internal collaboration and coordination are hindered. • Inability to connect with customers, suppliers, and partners. 3. **Data Access and Security Concerns**: • Business-critical data becomes inaccessible. • Heightened risk of data loss or cyberattacks. 4. **Revenue Impact**: • Online services, admission & registration and payment face significant interruptions. • Stakeholders' support delays result in lost business opportunities. 5. **Reputation Damage**: • Students lose trust in DAHU's reliability. • Public perception suffers, affecting reputation. 6. **Financial Consequences**: • High recovery costs for systems and infrastructure.
Likelihood of interruption to university:	Possible
Recovery timeframe: *(How quickly must this function be recovered to avoid lasting damage)*	7 Hours (Recovery should be completed within 3 hours to prevent lasting operational and reputational damage)
Resources required for recovery:	
Staff *(Numbers, skills, knowledge, alternative sources)*	**1. Staff Numbers**: **a.** One Network Manager **b.** One Security Administrator **c.** One Database Administrator **d.** Two Network Support Specialists **e.** Two Operations Staff

	2. **Skills**: a. Expertise in network management, IT infrastructure, and security. b. Knowledge of cloud services, databases, and data recovery tools. c. Familiarity with DAHU's IT architecture and business systems. d. Understanding of disaster recovery protocols and procedures. 3. **Alternative Sources**: a. Backup external consultants for specialized tasks. b. Access to third-party IT support services or vendors for rapid recovery.
Data / systems *(Backup and recovery processes, staff and equipment required)*	1. Redundant ISP, FIREWALL, and failover systems in place. 2. Regular testing of backup systems for network infrastructure. 3. Backup network hardware (routers, switches, firewalls). 4. Access to cloud-based or offsite services for internet failover.
Premises *(Potential relocation or work-from-home options)*	1. Employees can work remotely using VPN for secure access. 2. Critical systems are hosted on cloud on SaaS or IaaS
Communications *(Methods of contacting staff, suppliers, customers, etc)*	1. **Internal communication**: Email and Mobile (SMS, WhatsApp) 2. **External communication**: Contact suppliers/vendors through email and phone. In case of significant disruption, communicate with students via university social media and website updates. Refer to **Section 6: Contact Lists** for full contact information.
Equipment *(Key equipment recovery or replacement processes; alternative sources; mutual aid)*	**Key Equipment Recovery or Replacement**: 1. **Redundant network hardware** (routers, switches, firewalls) is available and can be quickly deployed. 2. Spare **network cables**, **power adapters**, and **access points**. 3. **Failover ISP** (e.g., SD-WAN, cloud VPN). 4. **External vendors** to source replacement parts: HP, Cisco, Cyberrom . 5. Use **cloud infrastructure** for recovery of online services (AWS, Oracle) 6. **Emergency power supplies** (e.g., UPS for remote workstations)
Supplies *(Processes to replace stock and key supplies required; provision in emergency pack)*	**Backup Network Hardware**: 1. **Power Backup**:

	Backup UPS **(Uninterruptible Power Supply)** for critical network devices to ensure continuity during power outages. 2. **Security Tools**: Backup **security certificates**, **firewall configurations**, to be readily deployable in case of network breaches or security issues. 3. **Documentation**: **Network diagrams**, **recovery procedures**, and **contact lists** is stored in an easily accessible for quick reference.

Priority:	**3**	**Critical function:**	**Blackboard availability**
Responsibility: *(Role responsible for leading on this activity, plus deputies)*			1. **Systems Administrator** 2. **Deputies**: **a. Operations Team** (for general support and coordination)
Potential impact on University if interrupted:			a. Disruption to online courses, assignments, and exams b. Negative impact on teaching, learning, and academic progress c. Loss of communication between instructors and students d. Increased stress and dissatisfaction among students and staff e. Potential delays in grading.
Likelihood of interruption to university:			Possible
Recovery timeframe: *(How quickly must this function be recovered to avoid lasting damage)*			**12 Hours** (Recovery should be completed within 4 hours to minimize disruption to teaching schedules, student access, and academic integrity.)
Resources required for recovery:			
Staff			One network manager.

(Numbers, skills, knowledge, alternative sources)	One Security Administrator One System Administrator One System Support Two technical Support
Data / systems *(Backup and recovery processes, staff and equipment required)*	**Access to Blackboard vendor support** – If the issue is software-related, reaching out to Blackboard support for assistance **Authentication systems** – Ensure user access control systems (e.g., SSO) are recovered, or alternative login is activated
Premises *(Potential relocation or work-from-home options)*	Work from home is applicable as it is SaaS based
Communications *(Methods of contacting staff, suppliers, customers, etc)*	**A. Internal communications:** or internal website to inform staff, students, and faculty about issues and progress, b. **public communications:** Use email, use the university website, or SMS to inform students of disruptions and recovery efforts c. **Helpdesk communication**: Use support ticket systems or hotlines to manage and resolve user issues during downtime d. **Vendor support communication:** Direct communication with Blackboard's technical support for system issues or outages
Equipment *(Key equipment recovery or replacement processes; alternative sources; mutual aid)*	Blackboard system is in SaaS, DR is involved in the contract
Supplies *(Processes to replace stock and key supplies required; provision in emergency pack)*	Courses backup based on the retention policy

Priority:	**4**	**Critical function:**	**Website availability**
Responsibility: *(Role responsible for leading on this activity, plus deputies)*			1. **Network Manager** 2. **Security Administrator** 3. **Web developer**

	4. **Deputies:** a. **Network Support Team** (for troubleshooting and recovery) b. **Operations Team** (for general support and coordination)
Potential impact on university if interrupted:	**1.Operational Disruption**: a. Admission service will be disrupted. b. Inability to interact with prospective applicants c. Staff and students face delays in accessing important information and services. **3.Data Access and Security Concerns**: a. Loss of access to crucial data hosted on the website. b. Increased risk of data breaches or cyberattacks if the website is compromised. **5.Reputation Damage**: a. Students, faculty, and potential partners lose trust in the reliability of the university. b. Negative public perception could affect applications, retention, and university rankings. **6.Financial Impact**: a. Significant financial impact due to Loss of online admission and payments.
Likelihood of interruption to university:	Possible
Recovery timeframe: *(How quickly must this function be recovered to avoid lasting damage)*	**8 Hours** (Recovery should be completed within 8 hours to avoid lasting operational, reputational, and financial damage.)
Resources required for recovery:	
Staff *(Numbers, skills, knowledge, alternative sources)*	**1. Staff**

	a. One **Network Manager** b. One **Security Administrator** c. One Web Developer d. One **Database Administrator** e. Two **Network Support Specialists** f. Two **Operations Staff** **2. Skills** a. **Network Management:** Experience with network management. b. **Website development** c. **Security Expertise:** Understanding of website security, firewalls, and protection from cyber threats. **3.Alternative Sources:** a. **External Consultants**: For specific tasks like cybersecurity audits or advanced technical support. b. **Microsoft support**: Microsoft partner for SharePoint related issues **Expertise in Web Hosting:** Knowledge of AWS infrastructure and website management. (SLA with AWS for Support)
Data / systems *(Backup and recovery processes, staff and equipment required)*	1. **AWS Cloud Backup**: Website data (including content, databases, and configurations) is backed up in **Amazon S3** or similar AWS services 2. **Backup Website servers.**
Premises *(Potential relocation or work-from-home options)*	**Critical systems** (website, database) are hosted on **AWS (IaaS)**, reducing physical infrastructure dependency.
Communications *(Methods of contacting staff, suppliers, customers, etc)*	1. **Internal communication**: Email and Mobile (SMS, WhatsApp) 2. **External communication**: Contact suppliers/vendors through email, ticketing system and phone. In case of significant disruption, communication with students will be via university

	social media, email, and some time the website if the website is partially available., Refer to Section 6: Contact Lists for full contact information.
Equipment *(Key equipment recovery or replacement processes; alternative sources; mutual aid)*	2- app servers 2 web servers 1 DB server
Supplies *(Processes to replace stock and key supplies required; provision in emergency pack)*	Source code backup

Priority:	**5**	**Critical function:**	**Shared Folder availability**
Responsibility: *(Role responsible for leading on this activity, plus deputies)*			1. **Network Manager** 2. **Security Administrator** 3. **Deputies:** a. **Network Support Team** (for troubleshooting and recovery) b. **Operations Team** (for general support and coordination)
Potential impact on university if interrupted:			1. Loss of access to critical data for staff and faculty. 2. Disruption to teaching, and administrative functions 3. Possible delay in services to students and staff 4. Negative impact on collaboration and communication within departments 5. Risk of data integrity or security issues
Likelihood of interruption to university:			Possible
Recovery timeframe: *(How quickly must this function be recovered to avoid lasting damage)*			**6 Hours** (Recovery should be completed within 8 hours to avoid lasting operational, reputational, and financial damage.)
Resources required for recovery:			
Staff *(Numbers, skills, knowledge, alternative sources)*			**1. Staff** a. One **Network Manager** b. One **Security Administrator**

	c. One Web Developer
Data / systems *(Backup and recovery processes, staff and equipment required)*	a. Access to recent backups of shared folder data b. Veeam Backup and replication as a tool for data recovery d. Access to shared drive or cloud storage management tools e. Cybersecurity tools to ensure data integrity and security during recovery
Premises *(Potential relocation or work-from-home options)*	a. Ability for critical staff to work remotely, if necessary b. Access to fileserver recovery sites, to restore service c. Access through File cloud
Communications *(Methods of contacting staff, suppliers, customers, etc)*	a. Internal communication platforms (email, message, WhatsApp) to notify teams of the issue b. Emergency contact list for affected stakeholders (IT, academic staff, administration) c. Use of collaboration tools (e.g., Microsoft Teams, Zoom) to maintain work continuity during recovery d. Communication with third-party vendors for backup or cloud disaster recovery.
Equipment *(Key equipment recovery or replacement processes; alternative sources; mutual aid)*	a. Backup servers, NAS (Network Attached Storage), DR cloud-based systems for restoring shared folders c. External tapes for backup data retrieval
Supplies *(Processes to replace stock and key supplies required; provision in emergency pack)*	a. Emergency IT equipment pack (e.g., cables, storage devices, portable tapes) b. Power backup systems (UPS) for critical IT infrastructure during outages c. Recovery software licenses in case of system restoration needs d. Physical or cloud storage for off-site backup access

5. Incident Response Procedure:

Task	**Completed** **(Date, time, by)**
Actions within 24 hours:	
Start of log of actions and expenses undertaken (see Action and Expenses Log)	
Liaise with emergency services (see Contact List – Incident Response Plan - Contact List)	

Identify and quantify any damage to the University, including staff, premises, equipment, data, records, etc	
Identify which critical functions have been disrupted (use Critical Function Checklist)	
Meet the responsible for recovering identified critical functions, and decide upon the actions to be taken, and in what timeframes (use Critical Function Analysis and Recovery Process)	
Provide information to: • Students, Faculty and Staff • Suppliers and customers • Related authorities	
Daily actions during the recovery process:	
meet those responsible for recovery to understand progress made, obstacles encountered, and decide continuing recovery process	
Provide information to: • Students, Faculty and Staff • Suppliers and customers • Related authorities	
Provide public information to maintain the reputation of the University and keep relevant authorities informed	
Following the recovery process:	
Arrange a debrief of all IT staff and identify any additional needs	
Use information gained from the debrief to review and update this business continuity management plan	

6. Contact Lists

This section contains the contact details that are essential for continuing the operation of the IT Department at the University. (Check the attached contact list)

7. Emergency Pack Contents

As part of the recovery plan for the IT Department, key documents, records, and equipment are held off-site at fileserver on cloud and hosted on cloud site in an emergency pack. This pack may be retrieved in an emergency to aid in the recovery process.

The contents of the emergency pack comprise the following:

a. **Documents:**

- A copy of this plan, including key contact details
- Related business continuity procedures and plans.

b. **Records:**

- Computer backup tapes and / or disks

c. **licences:**

- Licences, Contracts, and SLAs

8. Actions and Expenses Log

Date/time	Decision / action taken	By whom	Costs incurred

B. IT Disaster Recovery Plan

1. Purpose and Objectives:

a. Purpose:

To establish the **Disaster Recovery Plan** for the IT Department at Dar Al-Hekma University. This plan outlines the steps, roles, and procedures required to recover from disruptive events affecting IT services within the broader scope of the University's Business Continuity Management System (BCMS), which encompasses critical IT processes. It supports the restoration of essential operations. The goal is to restore essential IT services to an acceptable level as quickly as possible, while minimizing the impact of any disruption. The plan provides a framework for recovery based on predefined recovery objectives (RTOs and RPOs).

b. Objectives

- **Minimize Service Disruption**

  Ensure the continuity of critical IT services by reducing the impact of disruptions on operations.

- **Reduce Recovery Time**

  Implement effective recovery strategies to restore prioritized IT services within the defined Recovery Time Objectives (RTO), thereby minimizing downtime.

- **Enhance Operational Efficiency During Disruptions**

  Streamline processes and improve coordination across IT functions to maintain operational efficiency and service delivery throughout the disruption period.

2. Key Personnel and contact Information

These are the key resources involved in the disaster recovery plan, including all key stakeholders and third-party resources (Check the attached contact list)

3. Prioritized IT Services and Systems Recovery

a. Prioritized IT Services

The following table outlines the prioritized IT services, their **RTO (Recovery Time Objective)**, and the responsible personnel for recovery actions.

IT Service	**RTO**	**Responsible**
Management of Domain Controller and Active Directory	< 4 hours	Network Manager, Network Security
Management of File Server and Shared Folders	4 hrs – 1 Day	Network Manager, Network Security
Management of Internet Service	7 hrs – 1 Day	Network Manager, Network Security
Management of Data Storage	7 hrs – 1 Day	Network Manager, Network Security
Management of Local Area Network	7 hrs – 1 Day	Network Manager, Network Security
Management of Backup Systems	7 hrs – 1 Day	Network Manager, Network Security

b. Prioritized IT Systems / Applications

IT Systems / Applications	**RTO**	**Responsible**
VEEAM	< 4 hrs	Network Manager, Network Security
Management of Students Information System (SIS) Oracle Cloud Infrastructure and DR	< 6 hrs	System Administrator, DBA, Network Manager

Management of Blackboard	12hrs	System Administrator, System Support, DBA
Management of Website	8 – 12 hrs	Web developer, Network Manager

4. Employee Requirements

The following table outlines the recovery times for employees and their availability based on the nature and scale of the disaster.

Position	0 – 4 Hours	4 – 24 Hours
Director	1	1
Unit Head	2	2
Employees	2	5

All recovery team members participate in regular BCMS trainings and DRP awareness sessions to ensure understanding of their roles, response actions, and use of recovery tools.

5. Vital Records

Vital Records are critical to the recovery process. These records include:

a. **Standard Operating Procedures** for IT services.
b. **BCMS plans and recovery checklists** for IT operations.

6. IT Infrastructure Requirements

The following IT infrastructure resources will be required to continue operations during the recovery process.

IT Infrastructure Item	Quantity
Workstations and laptop	**7**
Internet Connectivity	Required

7. Key Suppliers

It is critical to maintain communication with key suppliers to ensure a smooth recovery process. All listed suppliers are evaluated annually based on their service-level agreements (SLAs), response capabilities, and recovery assurances to ensure alignment with Dar Al-Hekma's business continuity objectives. (Check the attached contact list)

8. Outage Scenarios and Recovery Strategy

Outage Scenarios and **recovery strategies** are designed to address various disruptive events, including:

a. **Unavailability of the Work Facility**: Teams will work remotely if the primary IT facility becomes inaccessible.
b. **Unavailability of Employees**: Employee availability will be confirmed, and alternate staffing or remote working arrangements will be made.
c. **IT Services Outage**: Restoration of critical IT services from backups or disaster recovery sites will be prioritized.
d. **Operational Disruption**: Workarounds will be implemented to ensure continued operation of essential functions until normal services are restored.

9. Disaster Recovery Procedure

a. Recovery of Work Facility

Step No.	Key Activities	Responsibility
1	Notify the Business Continuity Manager of team availability and await instructions.	Business Continuity Planner
2	Contact recovery team members to confirm their safety and availability.	Business Continuity Planner
3	Relocate to work from home alternative	IT Team
4	Check access to vital records and essential applications.	BCMS Team
5	Report any issues with applications, data access, or team safety to the BC Manager.	Business Continuity Planner
6	Confirm successful relocation to the BC Manager.	Business Continuity Planner
7	Provide regular updates to the BC Manager on recovery progress.	Business Continuity Planner

b. Recovery of Personnel

Step No.	Key Activities	Responsibility
1	Review staff roles and alternates; confirm availability.	Business Continuity Planner
2	Inform the BC Manager about team member availability.	Business Continuity Planner

3	Notify the BC Manager of any personnel that need to be relocated and the required number.	Business Continuity Planner
4	Continuously update the BC Manager on staff recovery progress.	Business Continuity Planner

c. Recovery of IT Services

Step No.	Key Activities	Responsibility
1	Assess the status of IT systems and data center recovery with the BC Manager.	Business Continuity Planner
2	Upon confirmation of DR site activation, check access to critical systems.	Business Continuity Planner
3	Report any system or access discrepancies to the BC Manager.	Business Continuity Planner
4	Confirm system recovery with the BC Manager if no issues are found.	Business Continuity Planner
5	Report on access problems with the Business Continuity Planner and await further instructions.	Disaster Recovery Team
6	Notify the Coordinator once systems are accessible.	Disaster Recovery Team
7	Regularly update the BC Manager on IT services recovery status.	Business Continuity Planner

d. Recovery of Cyber Incident

Step No.	Key Activities	Responsibility
1	Containment of an effective system	Cybersecurity Administrator, Network Manager.
2	Restoring systems from a clean backup, or shift to DR.	Cybersecurity Administrator, Network Manager.
3	Replacing corrupted data from a clean backup.	Cybersecurity Administrator, Network Manager.
4	Installing patches.	Cybersecurity Administrator
5	Changing passwords, and improving network perimeter and host-based security	Cybersecurity Administrator, Network Manager.
6	Communicating with interested parties about changes related to increased security.	IT Department

7	Increasing network and system monitoring activities (short or long-term).	Cybersecurity Administrator, Network Manager.
8	Increasing internal communication/reporting related to monitoring.	Cybersecurity Administrator, BC Manager
9	Engaging a third party for support in detecting or preventing future attacks	Cybersecurity Administrator, NCA

e. Recovery of Business Operations

Step No.	Key Activities	Responsibility
1	Identify and initiate manual workarounds for affected processes.	Business Continuity Planner
2	Assess workaround options for potential security risks or operational flaws.	Business Continuity Planner
3	Assist in developing and applying approved workaround procedures.	Disaster Recovery Team
4	Implement the workaround solution upon approval from the BC Manager	BC Team
5	Report access or implementation issues to the planner for further guidance.	Disaster Recovery Team
6	Provide continuous updates to the BC Manager on business operation recovery status.	Business Continuity Planner

10.Resumption to Normal Operations Procedure

Step No.	Key Activities	Responsibility
1	Review the safety of the work premises and ensure it is safe to return.	Support Services Department
.2	Inform the BC Manager once it is confirmed that the premises are safe to return.	Support Services Department
3	Check if the IT facilities are operational and available at the building.	IT Team
4	Inform the BC Manager once the IT facilities are operational in the primary site.	IT Team
5	Notify the division heads on the readiness of the premises (IT facilities) to resume normal operations.	BCM Manager
6	If all is satisfactory, instruct staff to begin moving higher-priority processes back to the primary site, followed by lower- priority processes.	Business Continuity Planner

7	Update the BC Manager on the status of the resumption process.	Business Continuity Planner
1.9	Conduct a root cause analysis for the disruption and implement corrective actions to prevent similar incidents in the future.	BC team
1.10	Prepare a detailed incident report documenting the recovery process and circulate it among the team for review and feedback.	BC team – Process owner – BC Manager

This plan is reviewed annually or after any significant disruption, test, or organizational change. Updates are documented and communicated to all stakeholders.

Key Responsibilities for Resumption Procedures:

Role	Responsibilities
Business Continuity Manager (BCM)	Overall coordination with top management and BC Planner, approval of recovery steps, approve incident report.
Business Continuity Planner	Lead the recovery of IT systems, staff, and operations. Maintain communication with the BCM and coordinate team activities
IT Team	Ensure IT facilities and services are restored to normal operations
Support Services Department	Review the safety of the premises and coordinate the movement of staff to remote working.
Process owner	Document the incident report.

11.Scenario-Based Testing

The IT Department conducts annual scenario-based testing of this Disaster Recovery Plan, including tabletop and live simulation exercises. Tests validate recovery times, communication effectiveness, and plan coordination. Post-exercise reviews are documented, and plans are updated accordingly.