Business Continuity Plan

v 1.0

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**13 Oct 2024**	Abdulrahman Al-Jamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

1. Introduction 4
1.1 Purpose 4
1.2 Use of the Guide 4
1.3 Control 4
2. Definitions 4
2.1 Business Continuity Guidelines 4
3. Overview of Jadarah Business Continuity Plan (BCP) 5
3.2 Risk Type 5
3.5 Testing and Maintenance 7
3.5.1 Methodology Test 7
3.6 Business Continuity Plan Approach 9
3.7 Business Continuity Plan Template 9
Physical Establishment 9
Technology 9
3. Business Continuity Governance 10
4.1 Company Policy 10
4.2 Business Recovery Team 10
4.3 Significant Business Disruptions (SBDs) 11
4.4 Employee Awareness 11
4.5 Communication with Employees 11
4.6 Warm Site 11
5. Glossary 12

Business Continuity Plan

1 1. Introduction

1.1 Purpose

The purpose of this document is to outline the requirements of the Business Continuity

Policy (BCP) for Jadarah for Debt Collection Company (referred to hereafter as "Jadarah" or "the Company"), with a focus on the Risk Management Department's (RMD) responsibilities to ensure uninterrupted business activities.

The Company has developed its Business Continuity Policy (BCP) to document guiding principles aimed at guiding risk management within Jadarah and managing it.

1.2 Use of the Guide

The contents of this document are confidential and intended for internal use only. Under no circumstances should the contents of this document be disclosed to any third parties without explicit written permission from the Risk Manager or the CEO. Jadarah should also submit the policy to the relevant authorities such as the Central Bank in the event of regulatory or legal requirements.

The Business Continuity Policy (BCP) will be reviewed annually or the requirements of this guide will be reviewed and amended according to regulatory and compliance requirements. The approval of the Business Continuity Policy (BCP) will be obtained from the Board of Directors, with the Risk Management Department being the custodian of the document within Jadarah.

1.3 Control

The Risk Management Department owns this document; therefore, all inquiries and issues related to the guide should be directed to this department. Each copy of this document will be numbered and distributed to relevant parties. Any changes, if any, will be monitored by the Risk Management Department and will not take effect until approved by the Board of Directors. These changes will be communicated to all relevant parties after approval.

2. Definitions

2.1 Business Continuity Guidelines

The ability of Jadarah to continue its daily operations, including acquiring new customers, managing relationships with current customers, investment decisions, customer service, complaint resolution, etc., with minimal possible disruption.

The ability of agents and distributors affiliated with Jadarah to accept subscriptions, redemptions, and other services with minimal disruption.

- Response Plan: Notifying relevant departments of business disruptions, issuing instructions for affected operations in accordance with business continuity guidelines, and maintaining records for registration or uploading as soon as the business disruption ends.

• Hot Sites vs. Warm Sites: When planning and setting up a Disaster Recovery (DR) plan, the presence of alternative sites for information technology operations is crucial. Disaster Recovery (DR) site options include hot and warm sites, each with specific features, functions, and costs.

Hot Sites A hot site is a full or partial duplicate of core IT operations, including complete computer systems and near-real-time backup of systems, applications, and data. The most expensive forms of replication software are used to keep the hot backup site synchronized with the primary site. The hot site is used when the company can afford less than one day of business downtime, typically switching over in less than an hour and sometimes faster.

Warm Sites It is best to understand a warm site as a hot site minus the data replication operations, meaning the warm site provides access to space, facilities, and equipment but requires the installation of current backup copies. Systems and services are brought online to become operational. The warm site is suitable for companies or institutions that can withstand one or two days of business downtime, representing the usual delay between a primary site failure and the appearance of a recovery site. Many large and medium-sized companies operate warm sites because their costs are much lower than hot sites, with the warm site being designated as alternative sites by the HR and management group and used for a maximum of two weeks. If business disruption exceeds two weeks, fully equipped ready-to-use offices will be leased.

Jadarah management has decided to implement a hot disaster recovery site in the Jeddah General Administration and a warm site in the branch.

3. Overview of Jadarah Business Continuity Plan (BCP)

3.1 What is Business Continuity Planning "BCP"?

Business Continuity Planning (BCP) is the comprehensive process of developing a set of approved approaches and arrangements to ensure the company's ability to respond to disasters and resume its vital business functions within the required time frame. Therefore, it is an ongoing process of planning, developing, and implementing disaster recovery procedures to ensure optimal availability of vital business functions. The primary goal is to reduce risks and costs for Jadarah, its employees, customers, and suppliers.

Jadarah's Business Continuity Plan "BCP" will cover the following:

- Technology's preventive strategy • Mitigating the severity of initiatives during business disruptions • Resource recovery strategy to restore Jadarah to normal business operations • Facilitating compliance with regulatory requirements
- Enhancing Jadarah's image and credibility with employees and customers.

Guidelines for Business Continuity Plan:

The Business Continuity Plan developed by Jadarah is based on the following principles: •

Feasibility - Applicable to maintain Jadarah operations • Profit / Gain Protection - Protecting

Jadarah's financial commitments • Continuation of New Business - Maintaining the ability to serve customers and generate new business • Brand Protection - Avoiding public embarrassment and loss of credibility.

3.2 Risk Type

Business units need to consider the risks of technical and environmental disruptions, including but not limited to: • Hardware failures (including scenarios where system processing capacity exceeds system capacity). • Software failure • Communication disruptions (including communication interruptions

between branches and headquarters) • Transportation disruptions • Power outage • Loss of physical workplaces • Natural disturbances (such as fires, storms, earthquakes, etc.).

3.3 Business Continuity Plan Methodology: The Business Continuity Plan methodology should include the following:

Phase One: Business Impact Analysis • Identify critical business operations, assets owned, and shared with supporting functions to conduct Business Impact Analysis (BIA) • Formulate Recovery Time Objectives (RTO) based on BIA, which can also be periodically optimized by comparing with sector best practices • Critical assumptions in disaster, so the framework is comprehensive enough to handle the most stressful situations • Determine Recovery Point Objective (RPO) regarding data loss for each system and develop a critical strategy to handle the concerned data loss. • Take alternative actions during the time when systems are unavailable, along with estimating resource requirements.

Phase Two: Risk Assessment • Assess structural risks based on a comprehensive analysis of business impact, provided that this assessment takes into account all business operations and is not limited to information processing facilities. • Risk management by implementing a suitable strategy / structure to achieve Recovery Time Objectives and Recovery Point Objectives agreed upon for Jadarah. • Impact on the recovery of vital business functions, including online customer system and customer information data and systems related to Jadarah. • The dependencies and risks associated with the use of external resources and support.

Phase Three: Identifying Options and Business Continuity Strategy The BCP Business Continuity Plan should develop beyond IT and must also include people, processes, and infrastructure. The methodology must ensure the safety of people in external branches / locations at the time of the disaster. Identify response measures based on specific categories of disasters. To access the specified business recovery plan, it must take into account the risk acceptance of the company, sector, and applicable regulations.

Phase Four: Develop and Implement BCP Business Continuity Plan • Business plans, i.e., specific response procedures for company operations, practical evidence (do and don't, specific section dedicated to individual business units), and test procedures • Establishing administrative succession and emergency powers • Compatibility and coordination of emergency plans with both the company and its service providers. • Recovery operations must not affect the recovery control environment.

Emergency plans are specific to each outsourcing arrangement based on the relative importance of the assistance activities of the company.

Regular updates are necessary to accommodate changes made by the company or its service providers. Examples of situations that may require plan updates include the acquisition of new equipment, updating operating systems, and changes in the following:

Employee Affairs Phone numbers or addresses Business strategy Location, facilities, and resources Legislation Contractors, suppliers, and major clients New or discontinued operations Risks (operational and financial)> **3.4 Documents Related to Business Continuity**

Document Name:

Description Business Impact Analysis Report: Details of Business Impact Analysis Training

Results and Identification of Recovery Time Objectives and Recovery Point Objectives for Various Business Units

Risk Assessment Report: Describes the results of a risk assessment process conducted to assess the suitability of the major threats faced by the company's business continuity program and to determine any business continuity plan threats that the company must prepare for and respond to.

Emergency Response Plan: Detailed procedures on how to respond to crisis such as fires, earthquakes, threats, etc.

Crisis Management Plan: Details of the crisis management team responsible for company Jadarah and instructions/procedures on how to manage the crisis.

IT Disaster Recovery Plan: Disaster recovery plan for IT components.

Departmental Recovery Plan: Functional recovery plan for departments.

In addition to the comprehensive Business Continuity Policy and Plan Maintenance

Procedures, these documents first summarize the foundation for designing Business Continuity activities, which fundamentally assess the current operational environment of the company's Jadarah. The assessment consists of:

1. Understanding and identifying important business units and the company's process and the timelines at which these processes must be recovered after a disaster (Business Impact Analysis).
2. Considering the various physical threats applicable to the company's readiness and their impact on the company (Risk Assessment) Based on the assessments conducted, Business Continuity activities were designed with the aim of responding to events, recovering to alternative locations, resuming operations, returning to primary locations, and returning to normal life.

3.4 Testing and Maintenance

Given the critical nature of the Business Continuity Plan, Jadarah Company participates in periodic reviews (on an annual basis), with all reviews being tracked, reviewed, and all review dates and announcements recorded for IT-related matters, Jadarah Company requests that the Head of the Information Technology Department be responsible for maintaining the annual schedule of all tests and reviews and all test and review records. The result of the periodic review will be communicated to the Risk Department.

3.5 Methodology Test

The Business Continuity Plan should be tested in the following ways: i. Component tests ii. Preferential exercise iii. Integrated simulation exercise iv. Complete simulation I. Component tests:

Component tests are tests of individual components of the comprehensive Business Continuity Plan. Four types of component tests must be conducted.

-Test type Purpose Confirming Plan Availability: To ensure that all employees on the distribution list have access rights to the latest version of the plan in hard copy.

- Retrieve vital records for printed copies from off-site locations To ensure that all vital records (copies of contracts, agreements, insurance policies, floor plans, property deeds, general partnership bonds, and limited partnership bonds) stored in an off-site location are already available, sufficiently updated, and retrievable within the expected timeframe.

- Contact with key employees, customers, and investment portfolio companies: To ensure that contact telephone numbers in the plan are correct and current. To ensure that resources

(human, equipment, vendors) needed can be obtained whenever and wherever needed.

- Contact tree tests To verify that all contacts in the contact tree are accurate and accessible.

Contact Tree: A document that graphically depicts communication responsibilities and the communication order used to communicate with management, employees, customers, vendors, and other key contacts in emergencies, disasters, or severe business disruptions.

II. Preferential Exercise:

In a detailed exercise, the Risk Department and Business Recovery Team (BRT) gather to walk through the steps of each component of the Business Continuity Operations as documented in the plan. Participants in this exercise will be gathered in a meeting room and a disaster simulation described to participants. Participants are expected to verbally respond to events by describing the steps they will take to play their assigned roles in the recovery and recovery process.

III. Integrated Simulation Exercise:

Integrated tests are a set of multiple component tests combined in one exercise. The goal of this exercise is to familiarize stakeholders with the recovery process and identify any gaps in the "integrity" of the plan - in terms of how components communicate with each other.

IV. Comprehensive Simulation:

In a comprehensive simulation exercise, the primary facility will be rendered inaccessible and the organization will be tested for its ability to operate from the command center.

Annual Test Schedule It is important that the Business Continuity Plan BCP be regularly tested using the correct type of test. The following table describes the test schedule generally used: Test type Recurrence Component tests Semi-annual Detailed exercise Semi-annual Integrated simulation exercise Annual Comprehensive simulation Once a year or as required by regulatory authorities, whichever is earlier

3.6 Plan Maintenance:

BCP maintenance is done through two types: scheduled maintenance and unscheduled maintenance. Scheduled maintenance is time-driven, while unscheduled maintenance is event-driven.

A - Scheduled Maintenance Scheduled maintenance is conducted according to the review schedule and should be conducted every six months. The purpose of scheduled maintenance is to determine whether changes are needed to the contents of the Business Continuity Plan or not. Scheduled reviews are jointly conducted by members of the Risk Management Department and the Business Recovery Team (BRT). Input from other employees may be requested as needed. The Business Recovery Team (BRT) leads (leads) all scheduled maintenance meetings, with the Risk Management Department responsible for documenting and working on changes discussed/agreed upon in meetings. All changes to the Basic Business Plan document must be implemented by the Risk Department with the approval and approval of the relevant department.

The following aspects should be reviewed in scheduled maintenance reviews: • Important business processes and recovery time goals associated with them • Ensure that the central operating site for emergencies and assembly point locations is updated and available • All contact lists and contact lists (employees, vendors, etc.) and emergency telephone numbers are updated and ensure they are updated. • Technological changes and infrastructure at Jadarah Company and their impact on recovery and recovery plans • Vendor contracts and performance against service level agreements (if applicable). and: • Recovery options and corresponding actions and updates as needed.

B - Unscheduled Maintenance Unscheduled maintenance is changes made to the Business Continuity Plan document that are required by events or need to be urgently scheduled.

Events that may require unscheduled maintenance of the plan include: • Changes in the business process environment and / or workflow • Physical improvements or changes in workplaces • Transfer, upgrade, or resignation of individuals in the emergency notification list or Business Continuity Management coordinators • Changes in organizational structure. and: • Acquisition or merger with another company. • Significant improvement / weakening by an employee. The relevant risk department must inform unscheduled changes to the board of directors. The risk department is responsible for assessing the need for and integrating changes appropriately into the Business Continuity Plan document.

3.7 Business Continuity Plan Approach

The Strategic Recovery / Recovery Availability Approach divides the various risk mitigation activities into three main categories:

• Prevention Strategy - This requires taking prior measures to avoid and neutralize the impact of any disturbances, such as excessive training, network redundancy, system recurrence, etc.

• Mitigation strategy - This requires taking monitoring measures to prevent business interruptions, such as early warning systems and third-party agreements, etc.

• Recovery strategy - This requires taking post-facto actions to recover from disturbances, such as off-site backups, temporarily.

3.8 Business Continuity Plan Template

The implementation of the above business recovery strategy and operational components leads to the following Business Continuity Plan (BCP) model for the company:

3.9 Physical Establishment

- **Preventative Strategy:** Our preventative strategy focuses on securing our workplaces.
- **Mitigation Strategy:** Comprehensive insurance policies are taken to protect against any theft or destruction of physical facilities.
- **Recovery Strategy:** Not applicable.

3.10 Technology

- **Preventative Strategy:** The following tools are used as part of the preventative strategy: Information Systems:
    - Continuously improve, test, and update the business continuity operations model.
    - Continuously test detailed recovery plans.
    - Continuously improve and implement backup plans, including off-site media storage. Wired and Wireless Communication System:
    - Ensure and test backup communication between headquarters and branches. ○ Ensure internet connectivity and test using a warm site.

- **Mitigation Strategy:** Our mitigation strategy focuses on continuous monitoring for any possibility. The following tools are used as part of this strategy: Information Systems:
    - Monitor system capacity usage, error messages, and apply improvements. ○ Establish clear maintenance and support agreements with third parties.

- Continuously monitor appropriate backup implementations.
- Analyze, report, and issue recommendations after each disaster recovery test.

Wired and Wireless Communication System:

- Continuously monitor network capacity usage and apply improvements.
- Establish clear maintenance and support agreements with third parties.

- **Recovery Strategy:** Our recovery strategy focuses on: Information Systems:
  - Perform mirrored system and application backups for any updates on the following day they are upgraded on the production server. The server image is implemented and brought to the Disaster Recovery (DR) server, and the image is tested in Jeddah before being transferred to [City].
  - Restore data from daily backup sent to a warm site. Wired and Wireless Communication System:
  - Each Disaster Recovery (DR) team requires VPN connectivity to the warm site using redundant internet connections.

4. Business Continuity Governance

4.1 Company Policy

The company's readiness policy to respond to Significant Business Disruptions (SBDs) includes protecting employee lives and company assets, conducting financial and operational assessments, quickly recovering and resuming operations, and protecting all company data. If we determine we cannot continue our operations, we confirm to designated Jadarah Company employees their ability to access their work data.

Two important goals have been set by senior management at the IT level:

1. A one-day Recovery Time Objective (RTO): Meaning we tolerate a system downtime period of one day.
2. A one-day Recovery Point Objective (RPO): Meaning we tolerate the loss of transactions processed within one day.

Therefore, Jadarah Company management has decided to implement a warm disaster recovery site at the branch.

4.2 Business Recovery Team

The Risk Department has established a Business Recovery Team (BRT) based on critical functions. The Business Recovery Team members must facilitate risk identification and develop risk mitigation strategies across business areas.

Specific responsibilities for the recovery team during downtime include:

- Execute emergency response and employee evacuation.

- Notify senior management and activate (if necessary) recovery team members due to emergency situations or business disruptions.
- Pack and move to the designated alternate site for business recovery execution.
- Establish a livable work environment at the designated alternate site.
- Notify business partners and key third parties with new business contact phone numbers (as needed).

Coordination of Business Recovery Team: Function | Business Recovery Team Function

- Risk Manager Risk Leader and Coordination * Points HR Manager and

Administrative Affairs * HR Manager and Hotline Coordinator Collections Manager |

Collections Business Coordinator Finance and Operations Director, IT * Financial

Operations and IT Group Coordinator * Branch Manager | Disaster Recovery Site Coordinator IT Chief * IT Coordinator

4.3 Significant Business Disruptions (SBDs)

Jadarah Company plans for anticipating internal Significant Business Disruptions (SBDs) affecting its ability to communicate and conduct business, such as a fire occurring in our building.

4.4 Employee Awareness

In addition to familiarizing with the Business Continuity Plan (BCP) and understanding applicable roles and responsibilities, Jadarah Company requests all employees to remain vigilant regarding potential business threats and report any unusual circumstances. These circumstances may include unauthorized visitors to our office, unusual items left in designated areas, technology system issues, or smells or smoke.

The HR and Management Department will coordinate with the Risk Department to train the Business Recovery Team (BRT) and related recovery teams and response officials during a disaster in IT, and they will appoint team leaders within each recovery team responsible for notifying other team members.

4.5 Communication with Employees

In case of a Significant Business Disruption (SBD), the Risk Department will assess the best available communication method still accessible to the Business Recovery Team (BRT) and relevant teams to ensure all Jadarah Company employees are aware of Significant Business Disruptions (SBDs). The Risk Management Coordinator can quickly access all employees during Significant Business Disruptions (SBDs) through contact with the hotline coordinator. The available call tree with the hotline coordinator includes all office and mobile phone numbers for employees.

4.6 Warm Site

The warm site is a ready-to-use remote mirror system that accommodates all daily transactions, in addition to any service provided by the main site. According to Jadarah Company policy, 24 hours are allowed to promote the warm site's use in case of a disaster.

This warm site is not used unless access to the system at the main office is unavailable. Jadarah Company has established a mirror system at the branch that conducts any transaction of any type from clients or any service provided. With this setup, in case of main site failure, a warm site is provided, and all business transactions are directed to the other site for execution. Once the system is repaired, it synchronizes its database with transactions saved from the warm site. The reflected warm site must be well-maintained at all times, and continuous proper training must be conducted for all Jadarah Company members concerned to ensure each person understands the tasks assigned to him. In case of interruption, he will be well prepared to do so as required and expected.

5. Glossary

Alert: Notification of a possible imminent disaster or event. It usually includes instructions for individuals to stand ready for potential activation.

Alternate Site: A secondary operational site used by business functions when access to primary facilities is unavailable. 1) Another location or computer center or work area designated for recovery, 2) A location other than the main facility that can be used to perform business functions, 3) A location other than the usual facility used for data processing and/or performing critical work functions in the event of a disaster. Related terms: Hot Site and Warm Site.

Assembly Area: The designated area where employees and visitors gather if evacuated from the building/site.

Backlog: Uncompleted work that accumulates when a system or process is unavailable for an extended period and this work needs to be processed once the system or process is available again and may take a long time to process. In extreme circumstances, accumulated work may become significant so that the accumulated work cannot be liquidated.

Backup (Data): The process of copying data, electronic or paper, in some form to be available and used in case the original data is lost, originated from or destroyed, or destroyed.

Backup Generator: An independent power source, usually operating on diesel or natural gas or other.

Primary Site: Refers to the main headquarters building of Jadarah Company, the location where the company is currently operating.

Business Continuity: The organization's ability to deliver service and support its customers and maintain its profitability before, during, and after a business continuity event.

Business Continuity Coordinator: A role within a Business Continuity Management (BCM) program responsible for coordinating planning and execution for the comprehensive recovery of an organization or unit (units).

Business Continuity Management Program: A continuous management and governance process supported by senior management and resources to ensure necessary steps are taken to identify potential loss impacts, maintain implementable recovery strategies and plans, and ensure continuity of products/services through practice, review, testing, training, maintenance, and assurance.

Business Continuity Plan (BCP): A process of developing and documenting the arrangements and procedures that enable the organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after interruption.

Business Impact Analysis (BIA): A process designed to prioritize business functions by assessing the potential impact that may result if the company is exposed to a disaster.

Business Recovery Team: A team responsible for maintaining business recovery procedures and compliance with the company's Business Continuity Management program.

Call Tree: A document that graphically depicts communication responsibilities and the call order used to contact management and employees, customers, vendors, and other key contacts in emergencies, disasters, or outage situations.

Crisis Management: The comprehensive coordination of the company's response to a crisis in an effective and timely manner with the aim of avoiding or minimizing damage to the organization's profitability, reputation, and operational capability.

Damage Assessment: The process of evaluating the damage to computer systems, vital records, office facilities, etc., and determining what can be salvaged or restored and what needs to be replaced after a disaster.

Disaster: A sudden, unplanned catastrophic event that causes unacceptable damage or loss. This could be:

1. An event that affects the company's ability to provide critical functions, operations, or services for an unacceptable period of time.

2. An event that necessitates the activation of the company's recovery plans.

Emergency: An unforeseen or imminent situation that may cause injury or loss of life, destruction of property, or disruption of the company's normal business operations to the extent that it poses a threat.

Emergency Preparedness: The ability that enables a company or community to respond to an emergency in a coordinated, timely, and effective manner to prevent loss of life and minimize injuries and property damage.

Emergency Procedures: A documented list of activities to be immediately implemented to prevent loss of life and minimize injuries and property damage.

Recovery Site: A dedicated location for the restoration of business units, technology, or other operations considered critical to the company. Related terms: hot site, warm site.

Recovery Time Objective (RTO): The time period within which systems, applications, or functions must be recovered after a business disruption (e.g., one business day). The RTO is often used as a basis for developing recovery strategies and determining whether to implement recovery strategies during a disaster.

Recovery Point Objective (RPO): The maximum targeted period in which data might be lost from an IT service due to a major incident.

Structured Walkthrough: Types of exercises where team members actually execute business continuity plans and verbally review each step to evaluate effectiveness and identify enhancements, limitations, and gaps.

Vital Records: Essential records necessary for the continuation or reconstitution of the company during and after an emergency, as well as records essential to protecting the legal and financial rights of the company and individuals directly affected by its activities.