AMAAN
CAPITAL

Amaan Capital (Private) Limited Policies

FY 2023 -2024

February 12, 2024 – Contingency Plan Version 1.0

AMAAN CAPITAL (PVT.) LTD | 1, QASR-E-ZAINAB, CLUB ROAD, KARACHI, PAKISTAN

AMAAN CAPITAL

AMAAN CAPITAL (PRIVATE) LIMITED POLICY

Policy

Contingency Plan to Ensure Continuity of Operations in the Event of a Disaster or Crisis

Approved by

Board of Directors (Amaan Capital (Private) Limited)

Date of Approval

12 February, 2024

Effective Date

12 February, 2024

1. INTRODUCTION

1.1 This document defines the Amaan Capital (Private) Limited policies and procedures for Contingency Plan to Ensure Continuity of Operations in the Event of a Disaster or Crisis, as well as our process-level plans for recovering critical technology platforms and the communications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency, modifications to this document may be made to ensure the physical safety of systems, and data.

1.2 Our mission is to ensure information system operation, data integrity and availability, and business continuity.

1.3 The Securities and Exchange Commission of Pakistan (SECP) has prescribed macro-level principles of "Conflict of Interest" under regulation 16(10) of the Securities Brokers (Licensing and Operations) Regulations, 2016. Wherein, the securities brokers shall be required to take all reasonable steps including the framing of appropriate policies and procedures to minimize conflict of interest between the securities broker and its customers

2. POLICY STATEMENT

Management has approved the following policy statement:

2.1 The comprehensive IT Disaster Recovery Plan shall be reviewed annually.

2.2 A risk assessment shall be undertaken periodically to determine the requirements for the IT Disaster Recovery Plan.

2.3 The IT Disaster Recovery Plan should cover all essential and critical infrastructure elements, systems and networks, under key educational activities.

2.4 The IT Disaster Recovery Plan should be periodically tested in a simulated environment to ensure that it can be implemented in emergencies and that the management and staff understand how it is to be executed.

2.5 Staff must be made aware of the IT Disaster Recovery Plan and their respective roles.

2.6 The IT Disaster Recovery Plan is to be kept up to date to take into with changing circumstances.

3. SCOPE

The principal objective of the IT Disaster Recovery Plan program is to develop, test and document a well-structured and easily understood plan which will help Amaan Capital (Private) Limited recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and trading and settlement operations. Additional objectives include the following:

3.1 The need to ensure that employees fully understand their duties in implementing such a plan.
3.2 The need to ensure that operational policies are adhered to within all planned activities.
3.3 The need to ensure that proposed contingency arrangements are cost-effective.
3.4 Disaster recovery capabilities apply to staff, vendors and others.

4. KEY PERSONNEL CONTACT INFORMATION

4.1 Internal Contacts

NAME AND DESIGNATION	CONTACT OPTION	CONTACT NUMBER
First Level		
	Work	
	Mobile	
	Home	
	Email Address	
2nd Level		
NAME AND DESIGNATION	Work	
	Mobile	
	Home	
	Email Address	
3rd Level		
Head of Compliance	Work	
	Mobile	
	Home	
	Email Address	
4th Level		
NAME AND DESIGNATION	Work	
	Mobile	
	Home	
	Email Address	

4.2 External Contacts

NAME AND CONTACT	CONTACT OPTION	CONTACT
Building Authority		
Building In Charge / KElectric	Power Outage	118
Internet provider Primary Link		
	Work	
Internet provider Secondary Link		
	Work	
Software vendor		
	Work	
	Email Address	
Hardware vender		
	Work	
	Mobile	
	Email Address	
Other		
	Work	
	Mobile	
	Home	
	Email Address	

5. PLAN OVERVIEW

5.1 Plan Updating: It is necessary for the IT Disaster Recovery Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the Technology Department.

5.2 Plan Documentation Storage: Copies of this plan and hard copies will be stored in secure locations to be defined by the district. Each member of the IT Disaster Recovery Team will be issued a hard copy of this plan. A master-protected copy will be stored on specific resources established for this purpose.

4.2 External Contacts

NAME AND CONTACT	CONTACT OPTION	CONTACT
Building Authority		
Building In Charge / KElectric	Power Outage	118
Internet provider Primary Link		
	Work	
Internet provider Secondary Link		
	Work	
Software vendor		
	Work	
	Email Address	
Hardware vender		
	Work	
	Mobile	
	Email Address	
Other		
	Work	
	Mobile	
	Home	
	Email Address	

5. PLAN OVERVIEW

5.1 Plan Updating: It is necessary for the IT Disaster Recovery Plan updating process to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the training materials. This will involve the use of formalized change control procedures under the control of the Technology Department.

5.2 Plan Documentation Storage: Copies of this plan and hard copies will be stored in secure locations to be defined by the district. Each member of the IT Disaster Recovery Team will be issued a hard copy of this plan. A master-protected copy will be stored on specific resources established for this purpose.

5.3 **Prevention:** All attempts are made to prevent or limit the impact of a disaster on the information systems of our Company. Specifically, the following steps have been taken.

- All servers are in a centralized and secured location with access to limited staff.
- A separate independent cooling system is installed in the server room.
- All servers are password protected, with only a select person having rights to access the server.
- Uninterrupted power supplies are installed on all servers and key network equipment.

5.4 **Backup Hardware Strategy:** The key business server's backup strategy for each are listed below.

KEY BUSINESS SERVERS	BACKUP STRATEGY
Database Server	The same configuration server available with installations

5.5 **Backup Software Strategy:** Key business software's backup strategy for each is listed below.

KEY BUSINESS SERVERS	BACKUP STRATEGY
Database Server	Backup is available to restore within 30 min. Backup is available on-site and in safe remote locations.

5.6 **Risk Management:** There are many potential disruptive threats which can occur at any time and affect the normal trading process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency has been examined. The focus here is on the level of trading disruption which could arise from each type of disaster. Potential disasters have been assessed as follows:

Potential Disaster	Probability Rating	Impact Rating	Brief Description of Potential Consequences & Remedial Actions
Natural disasters (Flood, fire, earthquake, tornado, storms)	5	4	Backups of all servers are available in secure locations. Can be restored easily on new hardware.
Electrical power Failure	2	1	UPS array tested weekly. Building generator uptime less than 10 min.
Loss of communications network services	2	3	Network staff is available to troubleshoot and recover services.
Loss of Internet network services	2	1	A backup internet connection is available with an auto-switching option.
Communications network hardware failure	2	2	Device available in backup.
System hardware failure	2	2	Hardware/server is available in backup.

Probability: 1=Very High, 5=Very Low

Impact: 1= Minor annoyance, 5= Major Disruption

6. IT DISASTER RECOVERY PLAN EXERCISING

6.1 IT Disaster Recovery Plan exercises are an essential part of the plan development process. In an IT Disaster Recovery Plan exercise, no one passes or fails; everyone who participates learns from exercises what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that the emergency team is familiar with the assignment and, more importantly, is confident in their capabilities.

6.2 Successful IT Disaster Recovery Plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. The plan should also be validated by simulating the circumstances within which it has to work and seeing what happens.

6.3 Upon completion of the exercises, amendments to this document may be determined necessary. Revisions to this document will be noted on the cover sheet of the IT Disaster Recovery Plan.

7. IT DISASTER RECOVERY KIT AND SUPPLIES

An IT Disaster Recovery kit, including the following items, will be located at the Office and other safe locations.

7.1 Copy of the District's IT Disaster Recovery Plan

7.2 Copy of the telephone numbers and email addresses of all members of the IT Disaster Recovery Team.

7.3 Copy of telephone numbers with extensions and email addresses for all staff.

8. ANNUAL REVIEW

Amaan Capital (Private) Limited will review and update the Contingency Plan to Ensure Continuity of Operations in the Event of a Disaster or Crisis annually.

Approved By

Mr. Aman Aziz Siddiqui
Chief Executive Officer
Amaan Capital (Pvt.) Limited