

VM Vita Markets Ltd

(Regulated by the Cyprus Securities & Exchange Commission)

BUSINESS CONTINUITY POLICY

Original Issue Date:	October 2018
Approver:	Board of Directors
Last Review Date:	March 2020
Next Review Date:	October 2020
Version	1

Business Continuity Policy

Introduction

VM VITA MARKETS LTD (hereinafter the “Company”) is an investment firm established in the Republic of Cyprus and authorised by the Cyprus Securities and Exchange Commission (the “CySEC” or “Commission”) pursuant to the Law 87(I)/2017, to provide one or more investment services to third parties or/and perform one or more investment activities in accordance with its Cyprus Investment Firm (“CIF”) authorisation.

The Company has established and implemented a Business Continuity Policy (the “Policy”), which has been approved by the Board of Directors.

This Business Continuity Policy (hereinafter the “Policy”) aims at ensuring, in the case of a major interruption / breakdown / incident, the preservation of essential data and functions, and the maintenance of investment services and activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of its investment services and activities.

The Policy is designed to prevent, manage and resolve crisis situations. The Policy aims at minimising the risk of forcing the Company to suspend its operations, minimising the possible effect of temporary suspension of the Company’s activities and letting the Company recover its normal course of business, which may slow down in a crisis situation.

Examples of events that could cause a disruption to the business include a fire, flood, earthquakes, powers outages, elements of nature and acts of God, acts of war, terrorism, riots, civil disorders, rebellions, epidemic/pandemic, IT systems failure/interruption (virus/corruption, sabotage or other reasons), key personnel are unavailable or missing, inability of key service providers to perform (or their failure)

A business continuity event is defined as any incident requiring the implementation of special arrangements within the Company to maintain or restore services.

A disaster is defined as a disruption of normal organisational functions where the expected time for returning to normality would seriously impact the Company’s ability to maintain Client commitments and regulatory compliance. The Company shall put together a recovery and restoration program designed to support a recovery effort where Company would not have access to its facilities and data at the onset of the emergency condition.

The Policy shall be reviewed and updated on a regular (annual) on-going basis and be approved, at all times, by the Board of Directors.

Objectives

- To ensure the life/safety of all Company employees throughout the emergency condition, disaster declaration, and recovery process.
- To re-establish the essential organisation related services provided by the Company within a reasonable timeframe.
- To suspend all non-essential activities until normal and full organisation functions have been restored.
- To mitigate the impact to Company's Clients through the rapid implementation of effective recovery strategies.
- To reduce confusion and misinformation by providing a clearly defined command and control structure.
- To consider relocation of personnel and facilities as a recovery strategy of last resort (disaster recovery site).



Continuity of IT systems

The IT Department shall establish procedures to ensure that in situations of an interruption to the Company's systems (trading, telephones, etc.) and procedures, the following are met:

- (i) Preservation of essential data and functions.
- (ii) The maintenance of providing its investment services and activities.
- (iii) At least the timely recovery of such data and functions and the timely resumption of its investment services and activities.
- (iv) The software and hardware systems used at the Company's premises are fully operational at all times and the possibility of downtimes is minimised.
- (v) Backed-up databases are stored on backup facilities and are available for restoration at any time. Copies of the backed-up databases are stored in a different location for safety and early recovery reasons.

The Company shall identify specific systems which shall be considered as core systems required to ensure business continuity. These systems shall ensure:

- (a) The continued and uninterrupted access to the internet.
- (b) The continued and uninterrupted operation of the trading platform.