



**RC 315714**

# **STANDARD UNION SECURITIES LTD.**

## **Business Continuity Plan.**

January 2021

## Background

The objective of Information Security, Business Continuity Management and Back-Up Arrangement (BCM) is to ensure the timely resumption and delivery of essential business activities in the event of service disruption by maintaining the key business resources required to support delivery of those activities. The primary aim of this policy is to create a plan for mitigating some of an organization's risks.

### SOURCES OF DISRUPTION

In the course of our business over the years, we have identified some common sources of service failure which includes:

**1. Internet failure :**

Since all our business operations are done online, internet has become a very critical factor in our day to day business operations. However, due to the peculiarities of our operating environment, the internet sometime fails resulting in our inability to carry out some of the required operations.

**2. System Failure:**

In some cases, software issues, or even hardware issues may affect our ability to attend to our clients. Some of these issues include Operating system crash, software failure or malfunctioning among others.

**3. Server failure from our OMS vendor:**

There is a possibility of system failure from our vendor even though not yet experienced; it is, however, considered a possibility. If this occurs, some parts of our business activities shall be disrupted.

## **PLANS TO MITIGATE ABOVE IDENTIFIED THREAT**

### **1. Internet failure:**

In order to avoid service disruption as a result of internet failure, we shall always subscribe to the services of two or more internet service providers in order to enable us switch to whichever is working at the time of any particular failure. This implies that we shall have more than one 4g routers that we can switch the entire network to whenever there is a down time from any of the providers.

### **2. System Failure:**

The IT department must be equipped with personnel that can attend to issues arising from computer hardware and software, in order to promptly fix the affected systems.

### **3. Server failure from our OMS vendor:**

We shall always have a disaster recovery site (a separate environment not hosted on the same server with the main software applications) where we can move the last database backup into in order to continue business operations without delay. This must be discussed with our vendor Programos, in order to work out the best model to recover from which ever failure that may occur in this regard.

**PREPARED BY:MR. ANTHONY OLUSEYE OJEWALE**

**APPROVED BY: Chairman, Board of Directors**

**DATE: February 22, 2021**