BUSINESS CONTINUITY PLAN

As part of our ongoing commitment to our clients, this will serve to provide you with an overview regarding the EUROCOMM SECURITIES LIMITED (“EUROCOMM”) Business Continuity Plan ("BCP").

Business Purpose
The Securities and Exchange Commission, NGX and NASD require member firms/participating institutions to create and maintain a business continuity plan. A business continuity plan is a plan that will enable the firm to continue its business operations in the event of a significant business interruption.

Business Continuity Components
EUROCOMM SECURITIES LIMITED has evaluated the impact of business interruptions resulting from various events including but not limited to loss of facilities and resources. The BCP was developed by identifying methods to protect and restore critical business processes, records, data and systems to allow customers to transact business. EUROCOMM relies on an internal database system for customer records, transactions and third party for custody of funds and securities and trading platform. The third party provider has a business continuity plan with system redundancy and back-up facilities.

The EUROCOMM SECURITIES LIMITED Business Continuity Plan addresses the following key elements:

- Data Back-Up and Recovery
- Identification of Mission Critical Systems
- Financial and Operational Assessments
- Alternate Communications with Customers
- Alternate communications with Employees
- Alternate Physical Location of Employees
- Impact of Critical Business Counter-Parties
- Regulatory Reporting
- Communications with Regulators
- Customers Access to Funds and Securities

Recovery Plan
In the event of a business interruption, EUROCOMM SECURITIES LIMITED has plans and teams in place to address the immediate response to the incident, the management of the situation from the time of the incident until the matter is resolved, and a business unit and information technology recovery plan.

The data recovery plan includes maintenance of redundant real-time system facilities. The staff and workspace recovery plan includes the relocation of critical personnel to alternate sites.

Whatever the event, our BCP is designed to enable the firm to be operational within 24 hours or less assuming that our backup device and third party providers systems are operational.

With the improvement of technology and cloud based environments, Eurocomm Securities Limited arrangement in the relocation of critical personal to alternate sites include the remote work locations arrangement and cloud based environment. Given that the NGX, NASD trading platform can be accessed from any location, personnel of Eurocomm can work remotely. Data are stored in the cloud with automated backup.

Updates and Information Requests
The EUROCOMM SECURITIES LIMITED BCP is reviewed and tested at a minimum annually. Modifications and updates are made to incorporate any material business change or regulatory requirement.

EUROCOMM SECURITIES LIMITED will continue to promptly post modifications and updates to the BCP

Disaster Recovery Policy

A *disaster recovery plan* is a document that defines the policies and procedures for dealing with various types of disasters that can affect an organization, especially the organization's IT (Information Technology) infrastructure. A *disaster* is any event that has a significant impact on an enterprise's ability to conduct normal business. This plan includes the information and procedures needed to resume an organization's operation after some sort of disaster. Sometimes the plan is split into several plans, one to address recoverable disasters (e.g., loss of a server) and a more comprehensive business continuity plan for use in total loss situations.

Some types of disasters we should specifically plan for include:

- Physical Break-ins: theft and/or destruction, terrorist attacks
- Remote attacks: attempts to steal, destroy, or corrupt data, theft of service, denial of service (DoS), computer viruses
- Hardware failures: servers, databases, networks, power outages
- Environmental disasters: fire, flood, hurricane, etc. (Generally all these result in power outages too)
- Accidents (human error): file loss, DB record loss, data corruption
- Other disruption: disgruntled employees, organized criminal activity, strikes, legal actions (e.g., shutdown orders), etc.

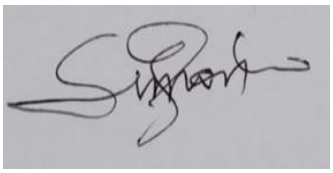
The staff should adopt the following plan and procedures in handling *of* disaster in the organization:

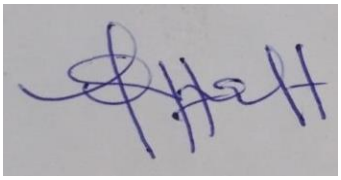
- Phoning the corporate attorney, The CEO (Ogbonnia Ojiako 08033035790) or board members (Ogbu Uchenna 08033035868), and others in the company, and let them follow-up.
- Store key data off-site. The location and access information must be documented in your DRP. Types of key data and documents to store off-line (and perhaps off-site) include system logs, backups, hardware inventories and configurations, network maps (showing connections, IP address assignments, DNS data, etc.), serial numbers for all equipment, software keys, licenses and permits, room keys (and combinations for locks), and any other security information (such as the *root* password for your servers).
- Keep paper copies of vital data (including your DRP).
- Keep information (contact information, passwords) current.
- Use *anti-virus* and *malware removal* software.
- Use and regularly test fire and smoke sensors and alarms, anti-theft systems.
- Have compliance assessments and evaluations (also known as *audits*) done at least once after any major IT infrastructure changes.
- Test disaster recovery plan by staging a *disaster drill*. Do every 1–3 years, more often if a lot has changed since the last drill (such as key personnel turnovers) or if your personnel need the practice. Tell people in

advance, and also fire, police, ISP, and others you are staging a drill at a specific time. Since you also should review the DRP every 1–3 years, it makes sense to do this test after the review, and possible changes.

- Maintain systems, including regular inspections (e.g., change A/C filters, examine fire extinguishers, and change batteries regularly in smoke detectors). Such disaster preventative measures should be clearly documented in your DRP, including who is responsible for doing what.
- Have a backup ISP, backup email and saving in the cloud
- Conduct training sessions.

APPROVED BY THE BOARD OF DIRECTORS





---------- ----------

Managing Director Director