Disaster Recovery Plan

CONTENTS

---

1. INTRODUCTION

The goal of Gilgamesh Financial Services and/or GFX Securities and/or the Company (the "Company") Disaster Recovery Plan (DRP) is to ensure business continuity in case of disaster/material business disruptions, as well as to protect data of the Company.

The Company considers that the ability to recover and restart its business including supporting technology if a crisis or disaster were to occur is critical to fulfilling its obligations.

Contents of the present document are confirmed by the Company's Board of Directors (the "Board"). Any changes, modifications, or alterations to this DRP will be reviewed and only approved by the Board.

The DRP of the Company sets forth the following goals:

- To minimize interruptions to the normal operations.
- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish alternative means of operation in advance.
- To train personnel with emergency procedures.
- To provide for smooth and rapid restoration of service.

---

2. OVERVIEW

The purpose of the Company's DRP is to ensure that in case of material business disruptions the Company resumes its operations with minimal interruptions and in the most efficient manner possible. The DRP covers all systems and functions critical for efficient operation of the Company.

The DRP, as well as any changes and/or modifications to DRP, are reviewed and approved by the Company's Board of Directors (hereinafter referred to as "Board").

Among other things, the Company will maintain and make available to all relevant employees the following information within the context of the DRP framework:

- Members of the Board/staff to be immediately contacted in case of an emergency along with their emergency contact information; [contact]
- Contact information for all liquidity providers and other critical business partners of the Company; [contact]

---

3. BACKUP SYSTEMS

The Company uses a backup trading server to ensure operations can be resumed as soon as possible in case the main trading server fails or needs to be shut down.

The Company has in place a data backup system that ensures all databases are fully backed up on a regular basis.

The Company also ensures that backup systems are in place to process client transactions and keep records pertaining to client accounts. These backup systems shall include:

- A phone trading procedure that enables clients to contact the Company via phone to receive information regarding the status of their trading accounts and/or place trading orders with the Company.
- Terminals that enable the Company's staff to directly access each liquidity provider's trading platform to inspect trading exposure and/or place trading orders with such liquidity providers.

The Company will monitor technological developments to keep such systems up to date at all times.

---

4. CONTINUOUS MONITORING

The Company systematically monitors its operational processes to timely detect various emergency situations. Such monitoring is overseen by the Risk Management department in cooperation with other relevant departments (IT, Administration, and Trade, etc.). Whenever possible, software monitoring and notification systems are used in this process along with regular manual inspection and reconciliation procedures.

Among other things, the Company monitors on a continuous basis the following:

- That technological systems and equipment used in the Company's operations are running properly and are not experiencing any malfunction or showing signs of degrading performance;
- That the liquidity feed provided by the Company to its clients duly corresponds to the aggregated liquidity pool available from its liquidity providers;
- That market exposure on the client side fully reconciles with market exposure on the side of liquidity providers.

The Company's Risk Management function assesses its business continuity procedures on a continuous basis and initiates modifications and/or amendments to such procedures whenever new relevant risks have been determined or new and more efficient methodologies of dealing with risks have been developed.

---

5. SPECIFIC CONSIDERATIONS

Potential situations identified by the Company as key operational risks and procedures to be implemented in case of such situations are as follows:

Trading server shutdown

In the event that server equipment processing the liquidity feed and/or trading orders of the clients' needs to be shut down during trading hours, shuts down or otherwise malfunctions:

1. The Company staff immediately notifies Administration and Trade department (hereinafter referred to as "Administration") and IT department;
2. If it is necessary to temporarily switch to accepting Client orders only over the telephone line, the Administration immediately notifies all clients by email and/or online platform notification of such switch;
3. If deemed reasonable, this notification is also posted on the Company's website;
4. The Administration continues accepting client orders via telephone line and executing them through alternative means of execution maintained by the Company;
5. The IT department ensures that the backup server is brought up securely and as swiftly as possible and notifies the Administration that the backup server is ready to process trading orders;

6. The Administration switches processing of the client trading orders to the backup server. Following that, the Administration notifies the clients (via e-mail and notification in the online platform) that trading has been resumed and removes notification of suspension in online processing of client orders from the Company's website;
7. The IT department ensures that the master trading server is brought back to operational condition;
8. The IT department and the Administration ensure proper synchronization of data (including trading balances and trading history) between the master server and the backup server for smooth continuation of processing of client orders;
9. When the master server is ready to be brought back into operation, the IT department along with the Administration coordinate return to processing of the client trading orders on the master server with as little disruption to trading activity of the clients as possible. This means that typically, the switch back to the master server will be conducted during market closure hours;
10. The IT department will keep the Administration informed on the matters throughout this procedure.

Erroneous Price Feed

In the event the Administration detects discrepancies between the price feed in the Company's platform and the aggregate pool of liquidity available from the Liquidity Providers, or a disruption in the price feed stream, the following immediate actions are taken:

1. The Administration immediately informs the IT department of the issue;
2. The Administration informs clients via electronic mail and platform notification tools about the errors in the price feed;
3. If it is possible to limit the issue to a specific liquidity provider, the stream from such Liquidity Provider is disabled by the IT department, and the Administration contacts the respective Liquidity Provider in order to resolve the issue as soon as possible;
4. If the problem cannot be resolved swiftly, the IT department in coordination with the Administration disables trading in financial instruments affected by the issue;
5. The Administration performs actions necessary to revert client trades based on erroneous price feed in a non-discriminatory manner, with the least possible disruption to the clients' trading process;
6. If erroneous price feed results in market exposure for the Company (e.g., a trade was executed at the end of the liquidity provider, but was not executed at the end of the client), the Administration performs necessary activities to close such market exposure as soon as possible through alternative means of execution (placing trading orders with liquidity providers via telephone, if necessary).
7. After immediate actions have been taken, the Board will oversee further resolution of the situation in close cooperation with the Administration and the IT department. In any case, throughout the resolution process the Company will ensure: 8. That any suspension of trading through the Company's services is as minimal as possible and covers the narrowest possible range of financial instruments; 9. That Clients are duly informed on any developments in the situation and any limitation in the Company's ability to provide services to them; 10. That all actions taken by the Company duly take into account market situation, including price feed provided by the liquidity providers.

Discrepancies in Market Exposure

In the event any discrepancy is found between aggregate trading exposure on the client side and that at the liquidity provider side, the following immediate actions are taken:

1. The Administration verifies that such discrepancy is indeed present;
2. The Administration verifies whether such discrepancy is due to: 3. A client having an open position which is not matched with the liquidity providers; 4. A liquidity provider attributing trading positions which do not correspond to trading exposure of the clients.
3. In the case described, the Administration performs steps necessary to liquidate (roll back) erroneous trading exposure on the client account(s) in the system and informs the client of such actions through e-mail and, if available, platform notification;
4. In the case described above, the Administration: 6.1. Swiftly contacts the liquidity provider to verify that trading positions have indeed been opened and that the liquidity provider does not immediately acknowledge those as erroneously opened positions; 6.2. Ensures that such communication is recorded or, if such a recording is not practicable, it is documented by the member of staff conducting such communication immediately in its aftermath (with the respective member of staff certifying correctness of the document with his/her signature); 6.3. If both premises stated above are true, the Administration closes the respective trading positions with the liquidity provider as soon as practicable (if possible, in the course of the same communication); 6.4. If it is not practicable to close trading positions with the liquidity provider as per above, the Administration opens a hedging market position with another liquidity provider as soon as practicable.

6. GENERAL

Regardless of specifics of the event, the Company's staff are required to adhere to the following principles while dealing with any emergency situation:

Priorities

In dealing with any emergency, the following priorities are to be observed:

1. Minimizing Downtime: Downtime of provision of services should be as minimal as possible. Services must be provided at least via telephone trading as soon as practicable.
2. Market Exposure: Market exposure on the Company's own account must be excluded or minimized in size and time length as much as practicable. When dealing with emergency market exposure on Company's own account, no member of staff must give consideration to trading performance of such exposure (profit or loss); all focus should always be on minimizing the quantitative and temporal extent of such exposure as much as practicable. For example, members of staff responsible for

covering the emergency exposure must not hesitate with such actions in order to obtain better pricing or in expectation of a respective market position bringing any profits on the Company's account.

3. Client Impact: Adverse financial consequences to the Company's clients must be kept as low as possible during any emergency. When implementing this principle, members of staff must adhere to the following:

   3.1. The first priority is to ensure that the Company, as much as possible, adheres to its business model and does not assume any market exposure on its own account or, when such exposure does occur due to an emergency, it is liquidated as swiftly as possible.

   3.2. Actual financial losses to the client accounts have precedence over any unrealized profits.

Time is of the Essence

In adhering to the aforementioned principles, time is of the essence. Within reasonable limits, swiftness of resolution of any emergency situation should have precedence over attempting to obtain ideal conditions of such resolution, and the fastest initial resolution/workaround for the emergency should be sought out first. For example:

1. Restoring Company's services in emergency mode in a shorter period of time has precedence over restoring them in full over a longer period of time.
2. Liquidating emergency market exposure at existing market prices immediately is preferable to liquidating it later at potentially more favorable prices.

Separation of Competence

Whenever dealing with an emergency situation, departments should operate within the frame of their respective competence and responsibility. Members of staff should not attempt to handle any tasks and/or decisions outside the competence of their respective position/department and should instead address the matter to the member(s) of staff with appropriate competence as swiftly as possible. To this end, emergency contacts for all relevant members of staff are always made available as per above.

7. COMPANY RECORDS

The records of trades placed on the trading platform are stored on the Company's internal servers. The Company will ensure continuous security of the data stored on the servers. The Company's primary systems will be stored in Amazon AWS. The Company is using Amazon AWS IT infrastructure, which is in line with the European Banking Authority Guidelines on Outsourcing (https://aws.amazon.com/blogs/security/aws-european-banking-authorityguidelineson-outsourcing/). Backups are done every day by closure of business

and are stored in a physical copy server (to be stored in Mauritius) and one reserve copy in another cloud service.

8. INVOKING DRP

It is the responsibility of customers to assume risks and possibilities of financial loss caused by failure of company systems:

- The failure of hardware, software, and/or internet connection;
- Wrong settings in the Customer Terminal;
- Update failure;
- Improper operation of the Customer's equipment;
- Ignorance or misunderstanding of applicable rules of the user guide.

The Customer acknowledges that during peak (highest) demand, difficulties may occur in communication with the Company's representative. The Customer acknowledges that under abnormal market conditions, the time for execution of Customer instruction may increase.

9. DRP TEAM ACTIONS

The Disaster Recovery Team shall be responsible for disaster recovery – determination, assessment, and recovery of the damage.

The Disaster Recovery Team must personally visit the office/branch office subject to disaster, make initial determination of the damage extent or technical outage, assess and establish a further recovery plan.

The Disaster Recovery Team shall determine the level of damage as per the table below and report it immediately to the Board of Directors:

- Minor damage:
  - Estimated downtime – less than 1 day;
  - Damage to either hardware, software, mechanical equipment, electrical equipment, etc.;
  - Processing can be restarted in a short time without any special recall of the personnel.
- Major damage:
  - Estimated downtime – from 2 to 6 days;
  - Sufficient damage to hardware or facility;
  - Selected teams will be called to take actions for restoring normal operations.
- Severe damage/Catastrophe:

- Estimated time for restoration – more than 1 week;
- Extensive damage or complete destruction of computer room or facility;
- Personnel will be called to implement the Company's Contingency Plan.

A member of the Disaster Recovery Team shall contact all employees and officers of the Company. In addition, certain third parties shall be contacted by a member of the Disaster Recovery Team as necessary. A list of all employees and third parties to be contacted will be maintained by each member of the Disaster Recovery Team both on and offsite.