INVEST M GLOBAL

DISASTER RECOVERY

PLAN POLICY AND PROCEDURE

FEBRUARY 2023

To Be Regulated by the Financial Services

Commission of Mauritius

1. Policy Statement

Invest M Global Ltd. (the "Company") has developed a Disaster Recovery Plan (DRP) to ensure that in case of a disaster or significant business disruption, business operations can continue and Company data can be protected.

The Company recognizes the importance of being able to recover and resume operations, including technology support, in the event of a crisis or disaster, in order to meet its obligations to stakeholders.

This DRP has been reviewed and approved by the Company's Board of Directors. Any changes, modifications, or alterations to the DRP must be reviewed and approved by the Board to ensure that it remains effective and up-to-date.

The goal of the DRP is to provide a comprehensive strategy for ensuring business continuity, minimizing disruption to operations, and protecting the Company's data in the event of a disaster or significant business disruption. The DRP outlines specific procedures and protocols to be followed in the event of such an event and includes measures for recovery and restoration of critical systems and infrastructure.

Invest M Global Ltd. is committed to maintaining an effective Disaster Recovery Plan and regularly reviewing and updating it to ensure that it meets the changing needs of the business and the evolving threat landscape.

The Disaster Recovery Plan (DRP) of the Company is designed to achieve the following objectives:

1. The primary objective of a DRP is to minimize the amount of time the business operations are disrupted due to a catastrophic event. The DRP aims to restore critical systems and applications promptly and provide alternate solutions to enable the continuation of business operations.
2. The DRP aims to ensure that critical data and systems are protected and can be recovered quickly in the event of a disaster or disruptive event. This can involve creating backups of essential data, storing them securely, and testing the ability to recover them.
3. The DRP prioritizes the safety and security of employees and customers in the event of a disaster. This involves creating evacuation and communication plans and ensuring the physical security of critical systems.
4. The DRP is designed to help the organization maintain compliance with relevant laws, regulations, and industry standards. This can involve creating a plan that addresses specific compliance requirements and regularly testing the plan to ensure its effectiveness.

The DRP is an essential component of the Company's overall business strategy, as it ensures that the business can continue to operate in the event of a catastrophic event. The plan is regularly reviewed, updated, and tested to ensure its effectiveness in response to evolving threats and changing business needs. The Board of Directors has approved the DRP, and any changes or modifications to it must be reviewed and approved by the Board to maintain its effectiveness.

2. Our Goal in DRP

Invest M Global Ltd. (referred to as the "Company") has developed a Disaster Recovery Plan (DRP) with the primary goal of quickly resuming operations in the event of any significant disruptions while minimizing any interruptions to the business. The DRP includes all the critical systems and functions that are necessary for the Company to function efficiently. The plan's purpose is to ensure that the Company can recover from any material business disruptions in the most effective way possible.

The Company's Board of Directors is responsible for reviewing and approving the Disaster Recovery Plan (DRP), as well as any updates or modifications made to the plan. The DRP is a comprehensive framework that covers all areas of the business, including technology support, data protection, employee and customer safety, and regulatory compliance.

As part of the Disaster Recovery Plan (DRP) framework, the Company will ensure that the following information is maintained and accessible to all relevant employees:

- A list of Board members and staff who should be contacted immediately in case of an emergency, along with their emergency contact details. This will ensure that the right people are informed promptly and can act quickly to mitigate any negative impact on the business.

- Contact information for all critical business partners and liquidity providers of the Company. This will enable the Company to maintain communication with its critical partners and providers during an emergency, minimizing the impact on its operations.

The Disaster Recovery Plan (DRP) is regularly reviewed and updated to ensure that it remains effective in the face of changing circumstances and emerging threats. The Company is committed to ensuring that its operations can quickly recover from any significant disruptions to maintain the continuity of its business operations.

3. Backup Option

In order to mitigate the potential risks of primary trading server failure or shutdown, Invest M Global Ltd. (hereafter referred to as "the Company") has established a contingency plan that involves the deployment of a backup trading server that can be activated swiftly to ensure business continuity. The Company has also implemented a comprehensive data backup system to ensure that all databases are backed up on a regular basis in their entirety.

To ensure that all client transactions are processed and client account records are maintained in the event of any disruptions, the Company has put in place backup systems. These systems comprise:

- Mobile System - This system allows clients to contact the Company by phone to obtain information about their trading accounts' status and place trades.

- Terminal/trading platform System - This system enables the Company's staff to access each liquidity provider's trading platforms, allowing them to monitor trading exposure and execute trades with the provider.

The Company is committed to staying current with technological advancements and will monitor them regularly to ensure that all systems remain relevant and up-to-date. This includes maintaining the backup systems' effectiveness and updating them as necessary to ensure they remain functional and available at all times.

4. Schedule Monitoring

To ensure the Disaster Recovery Plan (DRP) for an organization remains effective, it is important to continuously monitor and improve it. This involves several steps that include regular testing, reviewing and updating, tracking and evaluating, involving stakeholders, ensuring compliance, assessing and evaluating risks, and conducting regular audits.

One of the key steps is regularly testing the DRP to identify any weaknesses and areas for improvement. This can include simulating disaster scenarios to evaluate the response of the DRP team and systems. Through this testing, organizations can identify any shortcomings and take the necessary steps to address them.

Another important step is reviewing and updating the DRP on a regular basis. This includes updating processes, technology, and organizational structure to ensure that the DRP remains relevant and effective. It is important to track and evaluate the performance of the DRP to ensure it is achieving its goals. This includes tracking the response time of the team, the reliability of backup systems, and the accuracy of recovery procedures.

Involving stakeholders, such as employees, customers, and partners, in the monitoring process is critical to ensure the DRP remains effective. Regular training, updates, and feedback mechanisms can help stakeholders stay informed and provide valuable insights into the effectiveness of the DRP.

It is also important to ensure the DRP complies with relevant regulations and standards. This includes regularly reviewing and updating the plan to reflect changes in regulations and standards.

Assessing and evaluating risks to the organization and updating the DRP as needed to address new or evolving risks is another important step. This can include conducting risk assessments to identify potential threats and vulnerabilities and developing plans to mitigate them.

The Company's Disaster Recovery Plan will include systematic monitoring of its operations to promptly detect emergency situations. The Risk Management department, along with other relevant departments such as IT, Backoffice, and Trade, oversees this monitoring process.

The company utilizes both software monitoring and notification systems as well as manual inspection and reconciliation procedures. Some of the things the Company will continuously monitor;

The Company's monitoring process also ensures that the technological systems and equipment used in its operations are functioning correctly and are not experiencing any malfunctions or showing signs of declining performance;

The Company also monitors that the liquidity feed provided to its clients accurately reflects the aggregated liquidity pool available from its liquidity providers;

The Company also verifies that the market exposure on the client side is in full agreement with the market exposure on the side of the liquidity providers.

Finally, conducting regular audits of the DRP can help verify its effectiveness and identify areas for improvement. This can include both internal and external audits to ensure the DRP is meeting the needs of the organization and its stakeholders.

5. Sign of “Red-Flag”

The Company has identified potential operational red-flag situations and has established the following procedures to be implemented in the event of such occurrences:

A. Trading Server facing Problem

In case of server shutdown or malfunction during trading hours, the Company has a procedure in place and the action of the company will be as follows :-

- The staff will notify the IT and operations departments.
- Client orders will be accepted only via the telephone line, and clients will be informed through email and/or an online platform notification.

- The back office will continue accepting and executing client orders through alternative means.
- The IT department will ensure that the backup server is brought up securely and promptly.
- The Backoffice will notify clients once trading has resumed on the backup server.
- The IT department will work to restore the master trading server and ensure that the data is properly synced.
- Once the master server is ready, the IT department and Backoffice will coordinate a return to processing client orders with minimal disruption, typically during market closure hours.
- The management will report the situation to the relevant regulator for monitoring purposes, and the IT department will keep the management informed.

B. Price feed Inconsistence

If the Backoffice identifies discrepancies or interruptions in the price feed from the liquidity providers, the following actions will be taken:

- The Backoffice will promptly notify the IT department if there is a potential operational risk situation.

- Clients will be informed of any errors in the price feed through email and platform notifications.

- If the issue is traced back to a specific liquidity provider, the IT department will disable the stream from that provider.

- The Backoffice will contact the corresponding liquidity provider to address and resolve the issue.

- If the issue cannot be resolved quickly, trading in affected financial instruments will be temporarily disabled.

- The Backoffice will fairly and impartially reverse any client trades made based on the inaccurate price feed.

- The Backoffice will take immediate measures to minimize market risk for the company, such as executing orders through other means if necessary.

- Clear, concise, and frequent communication will be maintained with clients, providing regular updates on the situation and the progress of the resolution.

- Clients will be informed of any updates on the situation and any restrictions that may affect the Company's ability to provide services to them.

- The Company will consider current market conditions, including the price feed provided by liquidity providers, when taking any necessary actions to address the issue.

- The Board, Backoffice, and IT department will collaborate seamlessly to address and resolve the situation swiftly and effectively while minimizing disruption to the clients' trading activities.

C. Trading Exposure

If there are discrepancies in the trading exposure, the Backoffice will promptly investigate and verify the problem.

- The Backoffice will identify if the discrepancies are caused by a client open position that is not matched with liquidity providers, or if a liquidity provider is attributing trading positions that do not correspond to the clients' trading exposure.

- The Backoffice will take corrective action to reverse any erroneous trading positions on the client's account(s), and inform the client about the actions taken through email and platform notifications.

- If the problem is caused by a liquidity provider, the Backoffice will inform the liquidity provider to confirm the existence of the problem and ensure that any communication regarding the discrepancy is well recorded for future use and action.

- If both of the conditions mentioned above are met, the Backoffice will close the relevant trading positions with the liquidity provider as soon as possible, preferably during the same communication.

- Implementing automated alerts to notify the Backoffice of any discrepancies or unusual trading activity, allowing for prompt investigation and corrective action.

- If it is not possible to close the trading positions with the liquidity provider right away, the Backoffice will promptly establish a hedging market position with another liquidity provider.

D. Integrity and Competence

- Each department will carry out their tasks within their area of expertise and responsibility. Employees should not handle tasks or make decisions beyond their scope, and should instead direct the matter to the appropriate staff member with the necessary competence as quickly as possible. For this purpose, emergency contact information for all relevant employees is always readily available.

- Providing regular training to staff on how to identify and address trading discrepancies, as well as how to use the monitoring tools and alerts effectively.

E. Record Storing

The trading platform securely stores trade records on its internal servers, which are continuously monitored and protected by the Company. To ensure data security, the Company leverages Google's robust IT infrastructure, with primary systems hosted on Google storage cloud. In addition, daily backups are conducted at the close of business and stored on a physically secure server located in Mauritius. Furthermore, an additional reserve copy of the data is stored on a separate cloud service, providing redundancy in the event of a system failure or other unforeseen circumstances.

F. Disclosure to Client

The Company is obligated to inform customers about the potential risks associated with trading. As such, it is the responsibility of the customers to assume the potential risks and possibilities of financial loss resulting from unexpected events, such as:

- Market volatility: Trading in financial markets can be highly volatile and unpredictable, which can lead to sudden price fluctuations and losses for investors.
- System failures: Technical issues with trading platforms, software, hardware, or internet connections can result in lost trades or incorrect orders, potentially causing financial losses.
- Economic events: Political instability, changes in interest rates, or unexpected economic events can impact market conditions and lead to financial losses.
- Cybersecurity threats: Cyber attacks or other security breaches can compromise customer data or trading systems, potentially leading to financial losses.
- Customer error: Mistakes made by customers, such as entering incorrect orders or failing to follow trading rules and guidelines, can also result in financial losses.

G. Action Taken

When a disaster strikes, an organization's disaster recovery plan team takes charge of the recovery process. The team's actions depend on the specific event and the organization's disaster recovery plan. However, they typically follow a set of key steps to minimize the impact of the disaster and restore operations as quickly as possible.

- Activation of the disaster recovery plan: The team formally declares the start of the disaster recovery process and assigns specific responsibilities to team members.
- Assessment: The team assesses the extent of the disaster and the impact on critical systems and data. This includes identifying any damage or data loss, evaluating the availability of resources, and determining the recovery time objective (RTO) and recovery point objective (RPO) for each system.
- Prioritisation: The team prioritizes recovery efforts based on the criticality of systems and data. This ensures that the most important systems are restored first and that resources are allocated effectively.

- Notification: The team notifies relevant stakeholders, including customers, partners, and employees, of the situation and any steps being taken to restore operations. This helps to manage expectations and maintain open lines of communication during the recovery process.
- Implementation: The team carries out the steps outlined in the disaster recovery plan to restore systems, data, and operations as quickly and effectively as possible. This may involve restoring data from backups, replacing damaged hardware, or deploying alternate systems to maintain operations.
- Testing: The team tests systems and processes to ensure they are functioning properly before declaring the end of the disaster recovery process. This helps to identify any remaining issues and ensures that the organization is fully prepared for future disasters.
- Documentation: The team documents the disaster recovery process, including what worked well and what needs to be improved for future events. This information is used to refine the disaster recovery plan and improve the organization's preparedness for future disasters.

The disaster recovery plan team is responsible for ensuring that the organization is able to respond to and recover from a disaster, minimize downtime and data loss, and restore operations as quickly and effectively as possible.

The classification of the recovery may vary and depend on the following classification:

Level-1:
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;

Level-2:
Estimated downtime – from 2 to 6 days;
Sufficient damage to hardware or facility;
Selected teams will be called to take action to restore normal operations;

Level-3:
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.