I. DISASTER RECOVERY PROCEDURES

In preparation for an event that would partially or completely restrict access to the Firm's office due to a natural disaster, terrorist activity or other unforeseen event (referred to herein as an "**Event**"), the Firm's disaster recovery procedures are summarized below:

A. Workplace and Employees

1. All employees are aware of all exits from their relevant office. If there is an Event during normal business hours, employees will exit the office.

2. In case of an Event whereby employees are not able to reach their office, they should return to their home and await direction from the CCO. Communication will be in the form of either a telephone call or an email message. Employees are encouraged to work from home if they are unable to reach their office.

3. Should either office be closed for more than 24 hours, employees should work from home, unless the CCO of Quo Vadis decides to reassemble the staff (or certain members of the staff) at the Firm's other office location or at another back-up facility.

B. Event Communications

1. All employees are expected to keep at their residence a copy of the current Firm phone list. This list will be provided to employees of the Firm by the CCO and will contain the names and phone numbers of all employees with alternative contact information where available. During an Event, each employee will be contacted and notified of the appropriate next steps.

2. Further, as soon as reasonably practicable after an Event, all Advisory Clients will receive a communication (via email, direct mail or a phone call) from Quo Vadis informing them of the Firm's status, back-up plan and new contact information. The CCO will be responsible for handling or coordinating these communications.

C. Access to Data

1. Information Technology (IT) Provider

The Firm's IT provider is responsible for the Firm's cybersecurity and business continuity support.

2. Remote Access

Employees can remotely access Firm information, if necessary.

3. Employee Laptop and Mobile Devices

Firm employees are permitted to access work and work emails from personal laptops. Laptops are required to have Windows system passwords activated, and employees are required to have separate passwords for logging in to all work applications. Employees should use "Two-Factor" authentication whenever possible for added security.

Employees are also permitted to access their work email from their personal mobile devices. In the event that a device is lost or stolen, as previously mentioned, Outlook Exchange Server can wipe employee email from the device.

4. Trading Continuity

In the event of a platform disruption, trades can be placed over the phone with the Firm's approved brokers.

D. Cybersecurity

The CCO will maintain these cybersecurity policies in an effort to plan for and direct the appropriate staff of Quo Vadis to take reasonable steps to protect: (a) against attempts to gain unauthorized access to any Firm information or data, (b) sensitive or confidential data, (c) intellectual property, and (d) critical business systems.

As discussed in this Manual, the primary information technology assets used by the Firm are internet connections and cloud based software applications. It is worth noting that Quo Vadis generally relies on the information security and cybersecurity procedures of certain of its critical vendors to provide support in implementing its information security measures. On a regular basis the Firm will train its employees on its cybersecurity policies and procedures and best practices.

1. Applicability of Cybersecurity Policy

   These policies apply to any employee, contractor or third-party provider who is authorized to access Firm technology, information systems and/ or information assets ("**Covered Persons**" or "**Users**").

2. What Quo Vadis is Protecting

   It is the obligation of all Covered Persons to protect Quo Vadis technology and information assets. This information must be protected from unauthorized access, theft and destruction. Quo Vadis's technology and information assets are made up of the following components:

   - Firm laptop systems, application software (cloud based), system software (cloud based), etc.
   - System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
   - Application Software: used by the various employees of Quo Vadis. This includes any custom written software applications, and commercial off the shelf software packages.
   - Communications Network/Internet access hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

3. Access Rights and Controls

   A fundamental component of the Firm's policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental

meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the systems used by Quo Vadis Covered Persons. Access control is implemented by logon ID and password, and for some systems the use of additional authentication controls (i.e. "Two-Fact" authentication).

4. Connecting to Third-Party Networks

Quo Vadis will take reasonable measures to confirm a secure method of connectivity provided between the Firm and all third-party companies and other entities required to electronically exchange information with the Firm.

This policy relies on vendor management, including due diligence with regard to vendor selection, monitoring and oversight of vendors cyber controls, and data protection and confidentiality contract terms. As part of it vendor due diligence and oversight, Quo Vadis assesses vendor relationships and their cybersecurity controls as part of the Firm's ongoing risk assessment process.

As appropriate, based on user access and authorization, users will be trained on cybersecurity procedures and measures. Training will include how data breaches may result from unintentional employee actions such as misplaced laptops, accessing a client account through an unsecured internet connection, or opening messages or downloading attachments from an unknown source. Training will also include procedures for responding to cyber incidents under the Firm's Incident Response Plan, as described below. Training will emphasize and encourage responsible employee and vendor behavior and convey the Firm's belief that employees and vendors can be the Firm's first line of defense, such as by alerting Firm CCO to suspicious activity and understanding and following Firm protocols with respect to technology.

5. Incident Response Plan

Quo Vadis has outlined the following steps with respect to its Incident Response Plan for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of Quo Vadis's network. Some examples of security incidents are:

- Damage to a Quo Vadis computer system or network caused by illegal access. Releasing a virus or worm would be an example.

- Denial of service attack against a web server utilized by Quo Vadis. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.

- Malicious use of system resources to launch an attack against other computers outside of the Quo Vadis network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Covered Persons who believe their computer or a system, application or web-site used to conduct the Firm's business has been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the CCO immediately who will then consult with the vendor or other support as deemed appropriate and necessary. The Covered Person should not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the

security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.