TRADEWINDS
CAPITAL MANAGEMENT

C O N T I N G E N C Y P L A N

Tradewinds Capital Management, LLC (hereinafter referred to as "Tradewinds"), will utilize its access to technology, off-site record keeping and its key personnel to ensure that in the event of a loss, interruption of client service, if any, will be limited to the best of Tradewinds' ability. This Disaster & Business Continuity Plan presents our policies, procedures and obligations in the event of any of the following unforeseen events:

- Physical Losses (Emergency Dislocation of Office, Loss of Equipment, Loss of Communications);
- Business Operational Losses (Loss of Informational Resources, Loss of Substantial Third-Party Service Provider, Financial Loss);
- Loss due to Cyber-terrorism (Internet and Email Borne Viruses);
- Loss of Internet and Telephone Capabilities; or
- Loss of Key Personnel.

POLICIES AND PROCEDURES

1. Physical Losses

A. Emergency Dislocation of Office or Loss of Equipment

The first person who determines that an equipment loss or dislocation of the office has occurred shall be responsible for immediately contacting Bryant J. Engebretson, whose contact information can be found on the "contact list" attached to this Memorandum. If Bryant Engebretson is not available, the first person to determine a loss shall immediately contact Mark Anderson, thereafter, the order of contact is Kyle Jackson, Cindy Plagerman, Tressa Smith, Daniel Lewis, Sally Veum. Krista Williams, Shelley Klasse, and Ronald Cole. The individual who is initially contacted shall be the "officer in charge" until such time as Bryant Engebretson becomes available. Each employee should maintain an updated contact list, which itself shall be the subject of update and distribution as necessary to all Tradewinds personnel. Bryant Engebretson shall be responsible for updating and compiling the firm's emergency contact list.

Tradewinds has three primary concerns in the event that the offices are inaccessible (e.g., total loss of the building by fire, explosion, evacuation, flood, loss of power, etc.), equipment is lost (e.g., theft, failure of equipment or loss of equipment due to fire, flood, etc.) or communications suffer a disruption: (1) the records relating to firm clients; (2) the ability for the firm to continue to make and implement investment recommendations for its clients; and (3) the ability for firm clients to communicate with the firm.

(i) Backup procedures. All information stored on the Tradewinds computer shall be subject to weekly backups. All data files are backed up to a common network hard drive. Bryant Engebretson shall be responsible for performing the various activities that comprise the overall backup process and for ensuring the success of the backup.

(ii) Restoration of Data. In the event that the backup must be used to restore the lost data, the Bryant Engebretson or his designee shall be responsible for restoring the data onsite to the existing network file server. In the event of a complete loss, data restoration shall occur at a secondary location at the home of Bryant Engebretson. Tradewinds personnel will be responsible for coordinating the account information with the most recently received confirmations and trade information from the account custodians for each client account to ensure that any changes in the client accounts since the time the backup was performed have been addressed and the system updated.

(iii) Restoration Location. As discussed above, the secondary location from which firm personnel may restore the data and continue Tradewinds' operations and client service shall be the home of Bryant Engebretson.

Nonetheless, if files are lost, the regular and/or disaster recovery backups should afford an opportunity for Tradewinds to restore the majority of the information that comprises the lost materials.

B. Client Service/Client Communication

The officer in charge shall make it a priority to contact all Tradewinds clients and inform them of the loss and that these disaster/contingency plans are in place. At this time, the officer in charge shall endeavor to provide each client with contact information so that they may contact a representative of Tradewinds should the need arise. Similarly, all account custodians shall be informed of the loss and, if necessary, each custodian should be informed of the restoration location from which the firm will repopulate the network with the backup data. The officer in charge shall also coordinate with the account custodians and third party service providers (if any) to ensure that service from these parties is affected in the least possible manner.

To the extent that a total loss of communications results, including areas beyond the firm's offices, with or without an equipment loss, personnel shall report to either the firm's office or restoration location as designated by the officer in charge. The officer in charge shall then evaluate the situation and determine the best method to ensure client service and communication is restored in the most expeditious manner.

2. Business Operational Loss

There are three types of business operational losses against which Tradewinds must protect itself and its clients: loss of informational resources, loss of one or more substantial third-party service providers, and financial loss. To protect against such losses, Tradewinds has made a policy of choosing vendors with adequate disaster protection and/or diversifying vendors for informational resources and other third-party service providers. In addition Tradewinds will, to the best of its abilities under the circumstances, monitor and account for all company finances so that any financial losses suffered by Tradewinds will not adversely affect firm clientele.

3. Loss due to Cyber-terrorism (Internet and Email Borne Viruses)

Tradewinds considers the protection of client information and related data to be of great importance. To that end, the firm has established guidelines that seek to ensure computer security. In an effort to combat any Web-based attack, Tradewinds has established a security plan that includes anti-virus software and a firewall program. In addition, a password login that is individual to each firm workstation is required in order to gain access to the firm's network. These measures are intended to assist the firm with pursuing the identification of threats to client data located in the electronic arena. In the event, however unlikely, that an irregularity or threat within this area is identified, the procedures outlined in section (1)(A) regarding restoring from backup apply.

4. Loss of Telephone and Internet Capabilities

Telephone and Internet communications may rely upon land-based telephone lines. In an effort to mitigate the damage resulting from a loss of communications, the firm employs a non-integrated communication platform wherein internet services are separate from the firm's primary telephonic services. The firm has also employed cellular telephones for use in contacting clients as a contingency to the compromise of either service.

5. Loss of Key Personnel

The firm recognizes that Bryant Engebretson and Mark Anderson are "key" employees, for whose loss the firm must establish contingencies in an effort to prevent disruption to client service. Should Bryant Engebretson become unable to fulfill his obligations to the firm and clients, Mark Anderson shall serve as alternate, thereafter, Kyle Jackson, Daniel Lewis, Cindy Plagerman, Tressa Smith, Sally Veum, Krista Williams, Shelley Klasse and Ronald Cole shall serve.

POLICY REVIEW AND TESTING

The firm shall review and test the disaster/contingency plans found in this Memorandum annually to determine whether any modifications are necessary in light of any changes to the firm's operations, structure, business or location. While compliance with the law and with the firm's policies and procedures is each individual's responsibility, interpretive questions may arise. Please direct any questions related to this contingency plan to Bryant Engebretson.