Disaster Recovery

As part of its fiduciary duty to its clients, and as a matter of best business practices, CS Ellis has adopted policies and procedures for disaster recovery and for continuing CS Ellis' business in the event of an emergency or a disaster. These policies are designed to allow CS Ellis to resume providing service to its clients, in as short period of time as possible. These policies are, to the extent practicable, designed to address those specific types of disasters that CS Ellis might reasonably give its business and location.

Backgrounds

Since the terrorist activities of 9/11/2001, all advisory firms need to establish written disaster recovery and business continuity plans for the firm's business. This will allow advisers to meet their responsibilities to clients as a fiduciary in managing client assets, among other things. It also allows a firm to meet its regulatory requirements in the event of any kind of emergency or disaster, such as a bombing, fire, flood, earthquake, power failure or any other event that may disable the firm or prevent access to our office(s).

Responsibility

The principal is responsible for maintaining and implementing CS Ellis' Disaster Recovery and Business Continuity Plan.

Procedures

CS Ellis has adopted various procedures to implement the firm's policy and reviews to monitor and ensure the firm's policy is observed, implemented properly, and amended or updated, as appropriate, which include the following:

Recovery Policy

CS Ellis is responsible for documenting computer back-up procedures, i.e., frequency, procedure, person(s) responsible, etc. CS Ellis is responsible for designating back-up storage locations(s) and persons responsible for maintaining back-up data in separate locations. CS Ellis is responsible for identifying and listing key or mission critical people in the event of an emergency or disaster, obtaining their names, addresses, e-mail, fax, cell phone and other information and distributing this information to all personnel (see Emergency Vendor Contact List).

Policy
It is firm policy to maintain a current contingency plan/disaster response and recovery plan, always, and to ensure that firm personnel are trained to respond to any disaster in accordance with adopted procedures. In the event of a disaster, it is firm policy to safeguard employees, ensure that client account records are protected, to minimize risk to firm employees and facilities and to resume the business of the firm in as quickly and orderly a manner as possible.

Procedures

Death or Incapacity of Corporate Officer or IAR

Brett Pechersky is the individual for the assignment of duties in the event of death or unavailability of CS Ellis' key personal.

In the event of the death or incapacity of a CS Ellis' Officer or IAR, in a timely fashion the remaining Officers of CS Ellis will:

- Give clients notice of the demise/incapacity of the Officer/IAR
- Explain to the clients the redundancy in process and investment philosophy and assure clients that the same level of care and fiduciary duty will be practiced at the firm even in absence of the Officer/IAR.
- Assist clients in transitioning to Brett Pechersky (412) 401-0558 per our agreement or elsewhere, should the client decide to transfer assets to another firm.

Disaster Readiness

Offsite Maintenance of Disaster Recovery Plan
A current copy of these policies and procedures is distributed to each staff member at least annually. Staff members are required to keep the current version in an offsite location so that they will be accessible in the event of a disaster or other emergency.

Emergency Supplies
The Office Administrator is responsible for obtaining and maintaining in the office, appropriate emergency medical and other supplies for staff in the event exit from the building is delayed.

Protection of Electronic Data Systems
All firm employees are required to save their computer data to the Window's "Live Mesh" server and not to their individually assigned desktop computer's hard drive. This information is accessible from any computer that has 'synced' with the office PC or is also available from any internet connection remotely.

Furthermore, employees each have access to the cloud-based secure data depository at https://csellis.com. This is secure and redundant data file server accessible from anywhere with an internet connection.

Access to Client Account Data
If a disaster destroys the office computer system, all client portfolio records can be accessed remotely through internet connections with the client custodians and/or the firm's cloud-based file storage system.

Client Account Records

In the event hard copy records stored in the firm's offices are destroyed, the firm has verified with each client custodian that client account records will be made available to the firm online, for download directly from the custodian's database.

Protection of Hard Copy Records
It is the practice of the firm to scan and keep all relevant documents in 'soft copy' form to ensure proper back up and security of information. The firm uses a file synchronization process to the cloud-based secure file system.

Essential Firm Documents
CS Ellis maintains a binder containing copies of the firm's primary and essential business documents, including licenses, registrations, and other corporate documentation. Additional electronic copies of these documents are maintained by CS Ellis online at www.csellis.com.

Client Account Files
Soft copy documentation relating to each CS Ellis' client is maintained in an individual client account file. These account files contain new account documentation, client correspondence, client quarterly reports and other client documents. These documents are maintained on the firm's computer network and files are backed up electronically in the electronic storage back-up drive that is done weekly.

General Business Files
The Office Administrator maintains a current contact record of the firm's legal, accountancy, compliance and other professional advisors on the Custodian and Vendor Emergency Contact List (see attached).

Relocation of Operations / Temporary Facilities
To the extent possible, all firm operations will be moved to a suitable temporary location until the firm's offices are restored, or new office space is available. In the event this temporary location is impacted by the disaster and unsuitable for the relocation, we will attempt to move firm's operations to a location outside of the affected area.

Recovery Effort at Impacted Location
The Chief Compliance Officer will coordinate the firm's insurance claim with respect to the firm's impacted primary location and will coordinate the firm's business data and property salvage recovery operations.

Trading Resumption
Until full electronic trading capabilities are restored at the firm's primary offices or until they are fully enabled at the temporary facility, the portfolio managers will affect client transactions by telephone from their residences.

Coordination of Communications
All disaster recovery coordination will be conducted by the Supervisor or in his/her absence by the Chief Compliance Officer.

Communications with Employees
In the event of a disaster, all employees are required to call into the Staff Emergency Call-In Number 412-719-7958 within one hour of a disaster. In the event a staff member does not call in within one hour of a disaster, the Office Administrator, or other person designated,

will use the employee contact information to contact the employee and/or the employee's designated emergency contact.

Communications with Emergency Response Vendors
The Chief Compliance Officer is responsible for maintaining the current Government and Utility Emergency Contact list for the firm (see Emergency Vendor Contact List). The accuracy of the contact information on the current list is verified on a quarterly basis.

The Chief Compliance Officer or other designated staff will contact all necessary emergency response teams, which may include, emergency medical, police, fire, Penn Power, water department, telephone & internet service provider(s), property management company, casualty insurance provider and the like.

Chief Compliance Officer Communications with Clients

Prompt client communications are vital to reassuring clients of the safety of their assets and of the ongoing viability of the firm. The Chief Compliance Officer maintains a current list of contact information for all clients. Once staff safety issues are stabilized and the office premises are secured or an alternate location is established, the Chief Compliance Officer, and other designated staff will contact all CS Ellis clients, appraise them of the disaster recovery effort, and provide them with alternate contact information when available. Client contact will be via telephone, email, fax or mail as required by circumstances.

Communications with Vendors
The Chief Compliance Officer maintains a current list of contact information for all major vendors of the firm - the Vendor Emergency Contact List (form accompanying these procedures). The accuracy of the contact information on the current list is verified on a quarterly basis. The Chief Compliance Officer will prioritize vendor contacts as required.

Employee Training
The Chief Compliance Officer is responsible for training all existing and new trade staff regarding the firm’s disaster recovery procedures. Such training includes participation in building fire drills and overseeing the maintenance of emergency provisions in the office.

Emergency Vendor Contact List

Procedures

In the event of an emergency, the Chief Compliance Officer or other designated staff person will contact all necessary emergency response vendors.

Emergency Medical (Ambulance) / Fire / Police – Dial 9-1-1

Direct line to Fire Department – 724-863-7769
Paintertown Volunteer Fire Department

Direct line to Police – 724-863-1119
Penn Township Police Department

West Penn Power – 800-720-3600

American Funds
PO Box 2280
Norfolk, VA 23501-2280
800-421-9900

Charles Schwab & Co., Inc.
PO Box 982603
El Paso, TX 79998-2603
8777-774-3892