

Disaster Recovery

Policy

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

Background

Since the terrorist activities of 9/11/2001 and various catastrophic natural disasters, up to and including Hurricanes Katrina and Sandy, 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 an emergency or disaster, such as a bombing, fire, flood, earthquake, power failure, the loss of a key principal, or any other event that may disable the firm, key personnel, or prevent access to our office(s).

In response to the substantial and wide-spread damage caused by Hurricane Sandy in October 2012, the SEC, FINRA and CFTC communicated with a number of leading market participants to ascertain the storm's impact on various aspects of their operations. Following the issuance of a joint advisory by the SEC, CFTC and FINRA on August 16, 2013, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert focused specifically on business continuity and disaster recovery planning by investment advisers. While both the joint advisory and the Risk Alert identify the same six key areas, the SEC's alert provides more detailed guidance including (i) general observations and notable practices, (ii) weakness noted, and (iii) possible future considerations. Advisers should consider the following areas in their review of business continuity and disaster recovery planning ("BCP") practices: (1) preparation for widespread disruption; (2) planning for alternative locations; (3) preparedness of key vendors; (4) telecommunications services and technology; (5) communications plans; (6) regulatory and compliance considerations; and (7) BCP review and testing.

Responsibility

James S. Flower is responsible for maintaining and implementing Strategic Asset Management, Inc.'s Disaster Recovery and Business Continuity Plan.

Procedure

Strategic Asset Management, Inc. has adopted various procedures to implement the firm's policy and conducts internal reviews to monitor and ensure such policy is observed, implemented properly and amended or updated, as appropriate.

Basic elements considered while developing the Disaster Recovery plan included:

- | financial assessments and operations;
- | means of communication between and among managers, employees and investors;
- | the physical location of the parties;
- | the ability to evaluate the impact of an event on Strategic Asset Management, Inc.;
- | regulatory and reporting obligations; and
- | mechanisms to ensure the safety of assets and keep them preserved until they can be redeemed to ensure the orderly liquidation of the assets in the even that Strategic Asset Management, Inc.'s business cannot continue.

Overall implementation and monitoring of the firm's BCP is the responsibility of James S. Flower, supported by key personnel whose primary BCP roles and responsibilities have been defined. Where necessary and appropriate, Strategic Asset Management, Inc. may also utilize outsourced service provider(s) to assist in fulfilling one or more of the following functions:

Telecommunications Services and Technology

- | maintain an inventory of office equipment, including hardware and software; as well as key vendors. All such information is maintained in the Cloud;
- | server is maintained by Time Warner Cable and backed up to the Cloud. All personnel are authorized to contact Time Warner Cable and initiate procedures to restore server, if needed;
- | contact information for all employees is maintained in the Cloud and can be accessed by any employee on any mobile device; in the event of an emergency, all employees are authorized to contact clients, as needed, to inform them about the emergency. All employees can access a list of clients on the Cloud;
- | g-mail accounts for mission critical staff that will enable e-mail communications to continue in the event of internal systems failures;
- | all employees maintain personal electronic devices capable of accessing the Cloud, if needed;
- | both portfolio managers are able to trade, as needed, without access to the physical office.

Communications

- | proactively communicate with clients (either directly or via an e-mail blast) prior to a major storm to determine whether they have any transactions (e.g., cash raised, funds transferred, wire instructions executed, etc.) they will need executed if an extended outage occurs;
- | communicating the status of Strategic Asset Management, Inc.'s operations to clients through (i) recorded messages on the firm's main phone line; (ii) notifications posted on the firm's website; (iii) via e-mail blasts that include instructions for contacting the firm and employees who are working remotely; and/or (iv) through the use of third-party vendors in the event of a protracted disruption;
- | providing trading counterparties and key vendors with contact information; and
- | consider creating a Skype account and direct staff and clients to access this resource in the event of an emergency.

Alternative Locations

- | all employees can work from home, if homes are not available, can work from any location with internet access; and
- | paper copies of this business continuity plan are provided to all employees.

Preparedness of Key Vendors

- | annually Strategic Asset Management, Inc. will contact mission critical vendors and ask for their current disaster recovery plans. These will be reviewed by the CCO to determine if they are adequate to meet Strategic Asset Management, Inc.'s needs.

Regulatory and Compliance Obligations

- | update this procedure pursuant to any applicable regulatory requirements.

BCP Review and Testing

- | document any issues identified by persons working offsite, for example, during snow days and update plan if required;

- l review of Strategic Asset Management, Inc.'s Disaster Recovery Plan periodically, and at least annually, by James S. Flower or other applicable employee(s)

Key Personnel

In the event that one of the portfolio managers is incapable of performing his duties, the other portfolio manager will take over the responsibility for his clients.

Threat Awareness

James S. Flower will continue to be aware of resources available from federal and local governments to gather information about threat dissemination services that are targeted to the financial services industry and that provide threats to both physical and cyber security.