Aviance Capital Management
Focused Asset Management

Business Continuity Plan (BCP)

Adopted Effective January 1, 2017

Overview

This Business Continuity Plan ("BCP") outlines the immediate and long-term contingency planning and recovery process of Aviance Capital Management, LLC. The purpose of the BCP is to provide specific guidelines that Aviance will follow in the event of a failure of any critical business capability.

Aviance has developed additional succession procedures not contained in the policy in the event of an emergency that affects Aviance's key personnel.

Goals and Objectives

The goal of the BCP is to provide uninterrupted service to our clients and to minimize the disruption to business operations should a system or vendor failure occur. The BCP has been developed to meet the following objectives:

- Provide for immediate, appropriate and measured response to emergency situations;
- Minimize the impact upon the safety and well-being of firm personnel;
- Continue to provide an acceptable level of client services during any prolonged business interruption;
- Protect against the loss or damage to organizational assets; and

Provide our clients core services with minimum of inconvenience.

Risk assessment, disaster prevention, and disaster avoidance are critical components of Aviance's contingency planning process. The implementation of this BCP should help to ensure all data processing systems, data communication facilities, information, data and business functions can be restored in a secure manner. Restoration must be accomplished in a time frame consistent with legal, regulatory and business requirements while maintaining information integrity.

It is essential that our employees know what their responsibilities are in the event of a business interruption. Employees are required to read and review this BCP, at least annually. Employees are expected to be familiar with their responsibilities and understand how to execute required procedures. Employees should have access to this BCP and/or other written procedures as a resource during any business interruption.

Contingency and Disaster Recovery Team
Vendor Contact information is maintained in an excel spreadsheet on the network and updated regularly.

Contingency Policies and Procedures

The Chief Information Security Officer (CISO), Chief Executive Officer (CEO) and Chief Compliance Officer (CCO) or their respective designees will be responsible for assessing the extent of damage, verifying the usability of all essential services during any major disruption or emergency and, more importantly, for ensuring the completion of all detailed continuity planning by each line of business.

In order to maintain operations during the commencement of a significant emergency or disaster, Aviance will ensure all Employees are contacted to confirm their well-being and to provide information about altered work arrangements. Essential Employees will be notified via telephone, cell phone, or electronic mail with instructions on how and when to proceed to a known and agreed upon alternative site.

A. Physical Facilities and Alternative Work Sites

Arrangements will have been made to provide alternative physical facilities for key personnel to use in the event Aviance's primary facilities become unusable. If it is determined that the building occupied by Aviance is uninhabitable for any reason, an assessment will be made to immediately determine the nature and extent of the problem, emergency or disaster. In the event the building cannot be entered due to riot, fire, government action, extreme weather conditions or for any other reason, the following procedures are to be followed:

1) In the event of an emergency during regular business hours, the individual discovering the emergency should immediately contact the CEO and/or CCO or designee. Immediately thereafter, the CEO and/or CCO or designee will notify Employees about the nature of the emergency and will instruct Employees regarding appropriate action.
2) The CEO or designee will notify all other Employees that the building cannot be entered, and that an offsite emergency meeting will take place.
3) The nature of any further action will be determined during the offsite emergency meeting, including, if necessary, relocation of key Employees. In addition, key Employees have the ability to access nearly all of Aviance's electronic records and conduct securities transactions on behalf of Aviance's clients from offsite locations.
4) Every effort will be made to protect and preserve the original documents maintained in Aviance's primary office. Backup information files and copies of duplicate electronic

records will be retrieved and/or transferred to any alternative work site. Most records are available electronically and will be available via redundant IT systems.

B. Communications

In the event Aviance loses local telephone service, long-distance service or any other telecommunications services, then the following procedures will be followed:

1) The CEO and CISO or their respective designees will immediately ascertain the nature and expected duration of the outage.
2) If the outage appears significant and involves loss of local service or all long-distance service, it may force a relocation of key business and technology personnel to an alternative work site. The CEO or designee will use his/her cell phone to remain in contact with vendors and Employees.
3) If the outage is limited to the temporary loss of local or long-distance services, the CEO or designee will continually reassess the situation until service has been fully restored. Employees' personal cell phones should be used as an alternative to temporary losses of local or long distance service. The Chief Information Security Officer (CISO) or designee will direct the vendor to forward numbers to cell phones based on that assessment so incoming calls can be handled with limited disruption.

Aviance has created a master Employee phone list which includes the cell phone number of each of its Employees. In the event of a total phone system failure, Employees will utilize their cell phones to maintain contact with one another and operate the business where necessary. That list will be distributed to each employee as part of the new hire process, and will be updated and redistributed as new employees join Aviance.

C. Client Services and Recordkeeping

Aviance has developed the following procedures to ensure that client records and Aviance's records are safeguarded in the event of an emergency:

1) Aviance's server system is backed through a cloud-based server
2) Aviance maintains an Uninterrupted Power Supply (UPS) system in the event of a power failure.
3) Aviance maintains a degree of redundancy in its storage of physical documents related to clients.
4) Aviance maintains a contact list of the various brokers and vendors through which we do business. This list includes the company name, the name of the contact person that we use, and their contact information. This will enable us to contact the necessary people and resume our normal business activities even if our computers or offices are not accessible.

5) A copy of a list of Investors/clients and their contact information are kept at an off-site location as well as in electronic format on our network. Aviance may make use of off-site storage facilities for additional storage of certain records as deemed necessary.

D. Hardware/Software

The failure or temporary loss of certain of Aviance's hardware infrastructure or software applications will be addressed by the Chief Information Security Officer or designee. Aviance has determined that it is more likely for it to encounter sporadic hardware and software failures rather than a preponderance of such failures at one time. Aviance's CISO or designee consistently reviews the risk of failure with internal systems and has established processes to limit disruption.

If a failure of the internal system network is suspected, the Chief Information Security Officer or designee should immediately contact the vendor(s). Functionality tests will be performed to determine the extent of damage. If hardware has been damaged, the vendor will be instructed to repair the network or build a new one with similar capabilities.

E. Executing and Clearing Firms

Aviance does not maintain physical custody of clients' funds or securities, make markets in any securities, execute trades directly or participate in underwritings for clients. Each of these tasks is conducted by Aviance's executing and clearing broker-dealers/custodians. Each of Aviance's executing and clearing broker-dealers has developed contingency procedures to provide the above noted services in the event of a business disruption. Nevertheless, in the event of a disaster, the Chief Information Security Officer or designee shall be responsible for leading the efforts to remediate all problems.

Aviance maintains multiple trading relationships for best execution purposes. Those relationships also provide Aviance with the opportunity to respond to an outage at one or more of our trading partners so the firm may execute trades as necessary in our portfolios. Trading partners are based throughout the country, reducing the risk presented by the outage at a partner.

F. Testing and Evaluation

Employees are provided with a copy of Aviance's BCP upon commencement of employment and are notified when significant changes occur to the plan. The CISO or designee shall be responsible for answering questions about the BCP to ensure the success of the BCP in the event of a disaster.

The CISO or designee shall perform a formal review of this BCP and integrate any necessary revisions and updates based upon testing conducted during the previous year. The CISO

or designee shall take into consideration any recommendations from vendors, regulators and/or knowledgeable employees.

Aviance shall periodically test the BCP in order to evaluate its effectiveness. All tests shall be documented as to:

- when the test occurred;
- what tests were performed;
- the individuals that conducted the test;
- the results of the test;
- corrective action required as a result of the test;
- individuals assigned to implement the corrective action; and
- the anticipated date in which corrective action will be completed.

G. Exceptions

Although we attempted to anticipate the nature of certain business interruptions when creating this BCP, certain unforeseen circumstances may arise which may require us to deviate from the actions prescribed in this BCP. Specifically, in situations: 1) where following the BCP would place our employees in personal danger; 2) where following the BCP would cause us to be in violation of laws, rules or regulations; 3) where another action would be in the best interests of our clients; or 4) where such actions would be impractical. In situations where we deviate from the actions prescribed in this BCP, the Officer in Charge will document the deviation and include the reason.