

# Power Forward Management, LLC

## Business Continuity Plan (“BCP”)

### Firm Policy

Power Forward Management, LLC (“PFM”) is a registered investment advisor involved in the financial management of client accounts. PFM is committed to safeguarding the interests of its clients and customers in the event of any emergency or Significant Business Disruption (“SBD”). This BCP summarizes PFM’s efforts to mitigate risks inherent with unforeseen business interruptions. The BCP is designed to help protect PFM’s firm personnel’s well-being and property, make financial and operational assessments, quickly recover and resume operations, protect books and records, enable continuous management of client accounts, and allow its customers to transact business even in the event of an emergency or SBD.

### Significant Business Disruptions

SBDs can range from small interruptions such as power outages and severe weather to major catastrophes such as terrorist attacks, civil unrest, natural disasters, and infectious disease pandemics. These events could impact PFM’s ability to communicate with clients and essential service providers and disrupt the operation of securities markets.

### Office Locations

PFM has one office located at 1901 Avenue of the Stars, Suite 200, Los Angeles, CA, 90067.

In the event of an SBD, PFM will instruct firm personnel to work remotely from their personal residence or other secure location.

### Working Remotely

PFM’s Chief Compliance Officer (“CCO”) and/or senior management conducts an assessment at least annually to confirm whether firm personnel have adequate systems, equipment, and a secure and reliable internet connection to work remotely for an extended period of time. As part of the assessment, PFM confirms that firm personnel have remote access to critical trading systems, client data, and any other documentation or software necessary to perform their duties. If firm personnel have inadequate systems or equipment to perform their duties remotely, PFM provides firm personnel with the necessary resources.

While working remotely, firm personnel are encouraged to use their personal cell phones or voice over internet protocol (“VOIP”) technology to communicate with clients, service providers, regulators, and each other for the short-term or until a different phone system is established. In order to help safeguard client information on personal devices, PFM prohibits firm personnel from saving or accessing any client information outside of the secured environment provided by PFM or mission critical vendors.

### Disaster Recovery Team (“DRT”):

Name	Title	Cell Phone Number
Mike Power	Chief Compliance Officer	310-776-0407
Justin Stiegemeyer	Chief Executive Officer	818-984-3508

## **Responsibilities**

Each Disaster Recovery Team (“DRT”) member is responsible for understanding his/her role during an SBD. PFM’s CCO has the primary responsibility for implementation and monitoring of the BCP:

- Confirming PFM’s data back-up process (i.e., frequency, person(s) responsible, data backup location(s), etc.).
- Maintaining current contact information for firm personnel and critical service providers, including their name, address, email, cell phone and any other necessary contact information.
- Contacting firm personnel and relevant critical service providers in the event of an SBD.
- Designating and arranging recovery location(s) for firm personnel to meet to continue business.
- Assessing whether firm personnel have adequate systems, equipment, and secure and reliable internet at recovery location(s) and obtaining or arranging for adequate systems and equipment for these location(s), if necessary.
- Establishing a back-up phone/communication system to communicate with clients, service providers, regulators, and other firm personnel.
- Determining and assessing back-up systems and/or recovery plans for key vendors and mission critical service providers.
- Conducting periodic testing and training for key personnel.

## **When an SBD Occurs During Office Hours**

In the event of an emergency during office hours, call 911. The next appropriate course of action will depend on the nature of the emergency. Most types of emergencies will require all firm personnel to quickly evacuate the building, including fire, bomb threats, etc. If so, gather your belongings, if time safely permits, and promptly exit the building. Certain emergencies, however, may require that firm personnel remain in-doors, including the release of a hazardous airborne substance in the immediate vicinity of PFM’s principal office. Firm personnel should, at all times, follow the instructions of emergency personnel. All firm personnel are to meet at the designated area indicated below, if safe to do so, following any evacuation of the principal office.

Designated Meeting Area: Front of Building

## **When an SBD Occurs After Office Hours**

In the event of an SBD occurring after business hours, each firm personnel must be contacted, informed of the nature of the event, and given instructions regarding if, when, and where to convene. Any firm personnel initially discovering an emergency situation at the principal office must contact PFM’s CCO to inform them of the situation. If, for any reason, the CCO cannot be reached, firm personnel are to contact an alternative DRT member.

If, for instance, the disruption involves a power failure, firm personnel must first notify the CCO or a DRT member. That person shall contact the utility company to obtain an estimate of when power will be restored to the principal office. Once a plan of action has been decided upon, the CCO or DRT member will contact all firm personnel to notify them of the appropriate course of action.

## **Disruption in Services of Critical Third-Party Vendor**

In the event of a disruption in the services provided by a critical service provider, the CCO will contact the vendor to determine the nature of the problem and obtain an estimate of when services will be restored. If the vendor cannot be reached and services cannot be restored, the CCO will determine an appropriate “work-around” solution. PFM will also reference the vendor’s own recovery plan to attempt to determine likely causes of the disruption and the vendor’s estimate of the restoration of services therefrom. If continued efforts to contact the vendor and/or to restore services are unsuccessful, the CCO also saves all relevant files via cloud technology.

## **Client Access to Funds & Securities**

Client assets are held by Charles Schwab & Co., Inc. (“Schwab”). In the event of an internal or external SBD, if telephone service is available, PFM’s firm personnel will take client orders or instructions and contact Schwab on their behalf.

## **Data Back-Up & Recovery**

PFM maintains any physical books and records in a securely locked file in PFM's office locations. PFM's CCO shall be responsible for the retrieval of any physical files that may be necessary to continue business operations.

Books and records are scanned and uploaded electronically onto a secure cloud-based environment hosted by IBackup.com. All data is backed-up daily. This process is fully automated and is completed via a secure internet connection. In the event of an SBD that causes the loss of records, PFM will recover them from IBackup.com.

Email communication is hosted by Microsoft Outlook and can be accessed by firm personnel remotely.

Email communication is also available on our Network Solutions email system out of San Diego and additionally the Office 365 cloud both of which can be remotely accessed via home computers.

## **Financial & Operational Assessments**

In the event of an SBD, PFM will immediately identify what means will permit PFM's firm personnel to communicate with clients, critical service providers, regulators, and other personnel. Although the effects of an SBD will determine the means of alternative communication, the communications options PFM employs will include PFM's website, personal cell phones and secure email. In addition, PFM will retrieve firm records as described in the section above. In the event that PFM is put in a position to raise funds due to a credit issue, PFM will apply for a loan or credit line through one of the banking institutions it currently uses.

## **Mission Critical Systems**

PFM's "mission critical systems" are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities. These mission critical systems can be accessed remotely by firm personnel.

## **Internet Connection**

In the event PFM's internet is unavailable at an office location, firm personnel will be able to access Schwab's online system, as well as the website of regulators and service providers, remotely.

## **Telephone System**

In the event that PFM's local telephone service is disrupted, firm personnel are encouraged to use their personal cell phones to conduct business until service is restored.

## **Vendor Information**

A list of PFM's third party vendors and their relevant contact information is disclosed in Appendix B below.

## **Loss of Key Personnel**

If an owner is terminated, incapacitated, or fails to be competent in performing their duties, an emergency meeting will be held by the remaining owners to evaluate the situation and conclude on the best course of action. Shall the owner's clients be reassigned to another adviser representative; the client shall be notified in writing of the change along with any required disclosure documents. The remaining owners will also notify all proper regulators and vendors.

## **Disclosure of Business Continuity Plan**

PFM will provide a written copy of this BCP to clients upon request.

### **Updates, Testing & Annual Review**

All firm personnel will receive two (2) physical copies of PFM's BCP. One copy is to be kept at the firm personnel's work station. The other copy is to be kept at the firm personnel's home address. PFM will make updates whenever there is a material change to operations, structure, business or location, or to those of Schwab. In addition, PFM will test and review the BCP annually.

### **Chief Compliance Officer Approval**

I have approved the BCP as reasonably designed to enable PFM to meet its obligations to clients in the event of an SBD.

---

Chief Compliance Officer

---

Date