RRS' Business Continuity Plan (BCP) is designed to ensure we can continue to provide client support during a catastrophic event affecting our Deerfield Beach, FL, operations. The primary risk to RRS operations is hurricane activity from June to December. Other potential risks, though less likely, include fires, floods, tornadoes, and burglary. RRS management will reassess the BCP periodically throughout the year and as business conditions require. The RRS BCP addresses the following mission-critical factors:

CRITICAL BUSINESS OPERATIONS/PRIMARY RESOURCES

RRS management conducts periodic assessments of business operations to identify critical hardware, software, and physical location resources, providing a method for continued operations. The assessment considers the need for redundancies in operations, access to remote sites, and reliance on third-party providers for all mission-critical staffing, systems, physical locations, and data backups to ensure ongoing operations.

ONGOING MONITORING OF BUSINESS CONDITIONS

RRS continuously monitors critical hardware systems and software, third-party resources, and external factors. Monitoring of servers, network and internet access is conducted using SonicWall security services and Microsoft 365 Defender, which grants RRS remote systems management and real-time monitoring of all network and cloud resources to detect, prevent, and respond to cyberattacks or intrusions, or any other systems failures. RRS also monitors FINRA's critical sites for outages to ensure the systems will be available for filing purposes. Monitoring external factors includes real-time alerts from the National Weather Service, Securities and Exchange Commission, and, when available, the SROs.

The highest risk for outages is during the hurricane season, and our process for monitoring tropical disturbances begins when the National Weather Service releases its first notice of a potential tropical disturbance. When there is the potential for a storm to impact our operations within seven (7) days, we will notify all clients via email of the process that will be implemented in the event of an outage.

BACKUP AND REMOTE ACCESS

RRS employs a diligent backup system and is prepared to quickly redeploy assets to remote locations. All servers are backed up nightly on an incremental basis and a full backup is completed on a weekly and monthly basis. During storm season, client-critical files will be moved to Microsoft 365, One Drive, or SharePoint sites, hosted by Microsoft. In some circumstances, staff may be required to move business-critical files to encrypted portable drives to continue business operations on laptops from remote locations. Remote access to the primary server in Deerfield Beach is provided through a secure VPN connection configured with Multi-Factor Authentication. All mission-critical staff have access to the servers through this facility. RRS utilizes Microsoft 365 Enterprise and Azure cloud services for online storage of

corporate and client files (e.g., form filings, financial records, databases, active projects) during periods of anticipated outages.

To ensure that mission-critical systems are available—or can be quickly redeployed—RRS has a plan to deploy staff with necessary applications and client data to remote locations where access to regulatory and other information systems can be achieved. If necessary, RRS will relocate critical computer files to a remote "cloud server" for prolonged remote access. In the event of an actual or perceived extended outage in the Deerfield Beach offices, staff will be relocated as necessary to alternate locations.

In the event we are placed under a Tropical Storm Warning (*which means that tropical storm conditions are expected within the warning area within 24 hours*) or higher alert, we will likely suspend or limit operations until the storm has passed. This enables our staff to finalize preparations for the storm and seek a safe location. RRS senior management will determine the number of staff necessary to support operations and relocate them to one of the remote locations identified in the Remote Access section.

An outage in Deerfield Beach should not materially affect our telecommunications. Clients will be notified with remote telephone contact information. Email and FINRA applications are hosted by third parties that we will be able to access from alternate locations.

CALLING/COMMUNICATION TREE

In the event of a potential or actual closure of the Deerfield Beach office, the RRS calling tree will be implemented. Any staff member aware of an actual or potential office outage will contact the primary and secondary contacts via telephone, email, and/or text. The primary will contact the individuals in their contact group. If the primary is unavailable, the secondary will contact those individuals under the primary's tree in addition to their own. Once the nature and estimated duration of the outage is determined, RRS staff will contact affected clients. We will also attempt to post updates on our website at www.RRSCompliance.com.

Questions relating to our BCP should be directed to LouisDempsey@RRSCompliance.com or BartMcDonald@RRSCompliance.com, or (561)-368-2245.