Quad Cities Investment Group, LLC Business Continuity Plan ("BCP")

Firm Policy

Quad Cities Investment Group, LLC ("QCIG") is a registered investment advisor involved in the financial management of client accounts. QCIG 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 QCIG's efforts to mitigate risks inherent with unforeseen business interruptions. The BCP is designed to help protect QCIG'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, severe weather, and civil unrest to major catastrophes such as terrorist attacks, natural disasters, and infectious disease pandemics. These events could impact QCIG's ability to communicate with clients and essential service providers and disrupt the operation of securities markets.

Office Locations

QCIG has one office located at 5177 Utica Ridge Rd. Davenport, IA 52807. In the event of an SBD, QCIG will instruct firm personnel to work remotely from their personal residence or other secure location.

Working Remotely

QCIG'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, QCIG 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, QCIG 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, QCIG prohibits firm personnel from saving or accessing any client information outside of the secured environment provided by QCIG or mission critical vendors.

Disaster Recovery Team ("DRT"):

Name	Title	Cell Phone Number
Christine McElvania	Chief Compliance Officer	515-710-4024
Scott Stoltenberg	Partner	563-528-4391
Amy Kramer	Compliance Manager	563-210-5257

Responsibilities

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

- Confirming QCIG'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 and actual testing and training for mission critical and all 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 QCIG'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: Across parking lot in front of Biaggi's restaurant

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 the QCIG'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. QCIG 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 Raymond James financial Services, Inc. ("RJFS"). In the event of an internal or external SBD, if telephone service is available, QCIG's firm personnel will take client orders or instructions and contact RJFS on their behalf.

Data Back-Up & Recovery

QCIG maintains any physical books and records in a securely locked file in QCIG's office locations. QCIG'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 Office 365 SharePoint. 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, QCIG will recover them from backup source. Email communication is hosted by Office 365 and can be accessed by firm personnel remotely.

Financial & Operational Assessments

In the event of an SBD, QCIG will immediately identify what means will permit QCIG'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 QCIG employs will include QCIG's website, personal cell phones and secure email. In addition, QCIG will retrieve firm records as described in the section above. In the event that QCIG is put in a position to raise funds due to a credit issue, QCIG will apply for a loan or credit line through one of the banking institutions it currently uses.

Mission Critical Systems

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

Telephone System

In the event that QCIG'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 QCIG'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

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

Updates, Testing & Annual Review

All firm personnel will receive two (2) copies of QCIG'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. QCIG will make updates whenever there is a material change to operations, structure, business or location, or to those of RJFS. In addition, QCIG will test and review the BCP annually.

Chief Compliance Officer Approval

I have approped the BCP as leasonably designed to enable QCIG to meet its obligations to clients in the event of an SBD.

Chief Compliance Officer

Date

Appendix A Employee Contact Sheet

Christine McElvania

Phone: 515-710-4024

Email: cmcelvania@goqcig.com **Title:** Chief Compliance Officer

Laura Swift

Phone: 563-650-8268 Email: lswift@goqcig.com **Title:** Founding Partner

Jenny DeLaPaz

Phone: 563-343-5664 Email: jdelapaz@goqcig.com

Title: Partner

Jeremy Hauer

Phone: 309-230-6455 Email: jhauer@goqcig.com **Title:** Investment Advisor

Wayne Wagner

Phone: 563-343-4025 Email: wwagner@goqcig.com **Title:** Founding Member

Amy Kolner

Phone: 515-291-0243 Email: akolner@goqcig.com **Title:** Client Relations Associate

Scott Stoltenberg

Phone: 563-528-4391

Email: sstoltenberg@goqcig.com

Title: Founding Partner

Mark Grywacheski

Phone: 312-505-9341

Email: mgrywacheski@goqcig.com

Title: Partner

Amy Kramer

Phone: 563-210-5257 Email: akramer@goqcig.com **Title:** Compliance Manager

Angie McDonough

Phone: 563-579-3342

Email: amcdonough@goqcig.com **Title:** Client Relations Associate

Dave Borcherding

Phone: 563-505-0007

Email: dborcherding@goqcig.com

Title: Investment Advisor

Appendix B Critical Vendor Contact Sheet

Operational Contacts:

PHONE AND INTERNET COMPANY Central Scott Telephone Company

Contact Person: Tyler Bindrum 125 N 2nd Street, Eldridge, IA 52748

Phone: 563-285-9611

IT PROVIDER

Rouse Consulting Group

Contact Person: Help Desk 422 16th Street, Moline, IL 61265

Phone: 309-762-3589 Email: support@go2rcg.com

Data Back-Up & Recovery

IT PROVIDER

Rouse Consulting Group

Contact Person: Help Desk 422 16th Street, Moline, IL 61265

Phone: 309-762-3589 Email: support@go2rcg.com

Insurance Carriers

Nelson Brothers Agency

940 Lincoln Road, Bettendorf, IA 52722

Phone: 563-323-9233

Mission Critical Systems

Raymond James – RCS Department 880 Carillon Pkwy, St Petersburg, FL 33716 Phone: 727-567-7407 or 800-237-8691 Email: RCSservice@RaymondJames.com

Raymond James – Equity Trading 880 Carillon Pkwy, St Petersburg, FL 33716 Phone: 727-567-2000 or 800-564-3678

Email:

ECMAgencyTradeDesk@raymondjames.com

Raymond James – Mutual Fund Trading 880 Carillon Pkwy, St Petersburg, FL 33716

Phone: 727-567-3450

Email: MFTrading@raymondjames.com

Regulators & Compliance

Securities & Exchange Commission:

100 F Street, NE, Washington D.C., 20549

Phone: 202-942-0644 Phone: 1-800-732-0330 Fax: 202-551-8090

Or

Iowa Insurance Division

1963 Bell Avenue, Ste 100 Des Moines, IA 50315 Phone: 515-654-6600

FINRA:

1100 Poydras Street, Suite 850, Energy Centre

New Orleans, LA 70163 Phone: 240-386-4848 Fax: 504-522-6527 www.finra.org/index.htm

Advanced Regulatory Compliance:

Contact Person: Alex Butters 8383 Wilshire Blvd, Suite 950 Beverly Hills, CA 90211

Phone: 310-275-7300 Fax: 310-275-7305 Email: <u>alex@advreg.com</u>

Payroll & Benefits Providers:

ACCOUNTANT

Moorhead & Patterson

Scott Moorhead

3910 Lillie Ave, Davenport, IA 52806

Phone: 563-388-4744

Email: STM@MoorheadCPA.com

Legal Advice:

ATTORNEY

Pepping, Balk, Kincaid & Olson, LTD Jerry Pepping

105 7th Street, Silvis, IL 61282 Phone: 309-755-5096

Email: j.pepping@silvislaw.com

Appendix C Infectious Disease Pandemic Information

Restricted Office Access

In the event of an infectious disease pandemic such as COVID-19, QCIG will require all but site-critical personnel to work remotely until QCIG has determined local conditions have improved enough to permit firm personnel to return to the office. QCIG's CCO will notify firm personnel of any changes to office restrictions. While office access restrictions are in place, access to firm premises will be limited to site-critical personnel who must be physically located at their duty stations in order to perform their job. All other personnel must obtain permission from QCIG's CCO and/or senior management on a case-by-case basis before entering firm premises.

Firm personnel entering firm premises must practice 6-foot social distancing as much as possible, wear face coverings in all common areas, and wash their hands frequently. Janitorial staff will regularly clean and sanitize high traffic areas and touch points such as elevator buttons and interiors, door handles, handrails, light switches, faucets and restroom doors. QCIG will make adequate hand sanitizer and personal protective equipment, such as face masks, available for all firm personnel required to work on firm premises.

In order to help limit the spread of an infection disease during a pandemic, firm personnel are encouraged to conduct all meetings with prospective customers, current clients, regulators, and service providers via phone, video, or web conferencing whenever possible. Personnel should avoid entering into close proximity of clients who are senior investors and/or those who may have severe underlying medical conditions.

Protocol for Sick Personnel

QCIG's CCO and/or senior management has the right to send an employee home at any time if the employee appears to be sick or exhibit symptoms of an infectious disease. Personnel who are experiencing potential symptoms of an infectious disease should stay home in accordance with the current Centers for Disease Control ("CDC") guidelines. Anyone who has close contact with someone with an infectious disease should get tested before returning to the office.

Protocol If Personnel Test Positive for An Infectious Disease

Firm personnel who test positive for an infectious disease and have entered QCIG's premises within the exposure period as described by CDC guidelines should immediately notify QCIG's CCO and/or senior management of their test results regardless of their symptoms. QCIG's CCO and/or senior management may request a copy of the individual's test results for verification. If possible, the infected individual should confirm how recently they were on firm premises, whether they entered any common areas, and whether they were in close contact with any other individuals while on site.

QCIG's CCO and/or senior management will promptly notify any other firm personnel, clients, and/or others who have been in the same office or in close contact with the individual with an infectious disease within the exposure period as described by CDC guidelines. In accordance with federal privacy laws, QCIG's CCO and/or senior management must keep the identity of the infected individual confidential.

Employees located in the same office as an individual who tested positive for an infectious disease will not be permitted to return to the office for the exposure period as described by CDC guidelines or longer if they develop symptoms that do not improve. If safe to do so, employees should take any devices approved by QCIG's CCO and/or senior management for home use that are necessary in order to work remotely. Employees should monitor themselves for symptoms and seek testing depending on their healthcare provider's advice and availability of testing.

Any firm personnel who test positive for an infectious disease must request permission from QCIG's CCO and/or senior management prior to returning to firm premises.