1. INTRODUCTION:

As part of its fiduciary duty to its clients, and as required under SEC and/or FINRA Rules, Stonefield Investment Advisory (hereinafter, “SIA”) has adopted this Disaster Recover/Business Continuity Plan (hereinafter, the “Plan”) to provide for the firm’s recovery from an emergency or disaster and for the resumption of business operations in as short a period of time as possible. These policies and procedures are, to the extent practicable, designed to address those specific types of disasters that might reasonably face given its business and location. (See “TYPES OF DISASTERS- VULNERABILITY ASSESSMENT” attached hereto as **Appendix F**).

1. BACKGROUND:

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, pandemic or any other event that may disable the firm or prevent access to our office(s).

Our firm’s policy is to respond to a significant business disruption by safeguarding our employees and firm, assessing our finances and operations, communicating clearly with employees, clients, vendors, and regulators, recovering as quickly as possible, and continuing to transact business on behalf of our clients. If we are unable to continue our business, we will immediately allow our clients to access their funds and securities.

Jon R. Werner, Owner, is responsible for approving the plan and for conducting the required annual review. Our firm will update this plan when there is a material change to our operations, structure, business or location. Our firm will maintain electronic and hard copies of our BCP plan.

1. DISASTER RECOVERY TEAM:

Our firm’s two emergency contact persons are:

Jon R. Werner - Owner - Home: (319) 270-3462 Office: (319) 377-7811 x 2 Email: jwerner@stonefield.us

Rebecca Hanson – Office Manager - Home: (319) 640-9665 Office: (319) 377-7811 x 1 Email: becky@stonefield.us

[at least one must be a member of senior management and a registered principal of the firm if a broker-dealer]

Other members of the disaster recovery team are:

Jim Arenson - Attorney - Home: (319) 431-2057 Office: (319) 363-8199 Email: jarenson@arensonlaw.com

1. RESPONSIBILITIES:

Each employee is responsible for understanding his/her role during a disaster. The following individuals have the primary responsibility for implementation and monitoring of the Plan:

* Jon Werner is responsible for documenting computer back-up procedures, i.e., frequency, procedure, person(s) responsible, etc.

* Jon Werner is responsible for designating back-up storage location(s) and persons responsible to maintain back-up data in separate locations.

* Jon Werner is responsible for identifying and listing key or mission critical people in the event of an emergency or disaster, obtaining their names, addresses, e-mail, fax, cell phone and other information and distributing this information to all personnel.

* Jon Werner is responsible for designating and arranging for “hot,” “warm,” or home site recovery location(s) for mission critical persons to meet to continue business, and for obtaining or arranging for adequate systems equipment for these locations.

* Jon Werner is responsible for establishing back-up telephone/communication system for clients, personnel and others to contact the firm and for the firm to contact clients.

* Jon Werner is responsible for determining and assessing back-up systems and/or recovery plans for key vendors and mission critical service providers.

* Jon Werner is responsible for conducting periodic and actual testing and training for mission critical and all personnel.

1. WHEN AN EMERGENCY/DISRUPTION OCCURS:
	1. **Emergency 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 employees to quickly evacuate the building, including fire, bomb-threats, etc. If so, gather your belongings, including any medications, if time safely permits and promptly exit the building. Certain emergencies, however, may require that employees remain in-doors, including the release of a hazardous airborne substance in the immediate vicinity of the firm’s principal office. Employees should, at all times, follow the instructions of emergency personnel. If it is necessary to evacuate the building please refer to the “BUILDING EVACUATION PLAN” attached to this Plan as **Appendix D.** Please note key alternative routes in the event that main exit-ways are impassable during an emergency. All employees are to meet at the designated area indicated below, if safe to do so, following any evacuation of the principal office.

Designated Meeting Area: Jon Werner’s Home Address

* 1. **After-Business Hours Disruption/Discovery and Notification of Employees:**

In the event of a business disruption or disaster occurring after business hours, each employee must be contacted, informed of the nature of the event and given instructions regarding if, when and where to convene. Any employee initially discovering an emergency situation at the principal office must contact Jon Werner to inform him of the situation. If, for any reason, Jon Werner cannot be reached, the employee is to contact Rebecca Hanson or Jim Arenson and they will contact Jon Werner, if possible, and together the two will determine a course of action. (If, for instance, the disruption involves a power failure, the two will attempt to 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, Jon Werner shall initiate the Employee Call Tree. Jon Werner will attempt to contact the first employee on the “EMPLOYEE CONTACT SHEET” attached to this Plan as **Appendix A.**

If an employee cannot reach the next employee named on the call sheet, he/she will attempt to contact the next employee until he/she reaches an employee. Each employee notified must agree to contact the next employee on the list or continue down the list until an employee is reached. Each employee must keep track of the employees that could not be reached and inform the next contacted employee of these names. The employee reaching the end of the call sheet will attempt to contact the employees that could not be reached the first time until he/she either reaches an employee or fails to contact any of the remaining employees. When contacted, each employee is to be apprised of the situation and provided with instructions either to meet at the principal office at a later time, to meet at the alternative business location at a specific time or to await further instructions.

* 1. **Disruption in Services of Critical Third-Party Vendor:**

In the event of a disruption in the services provided by a critical service provider, Jon Werner or other designated individual will attempt to contact the vendor to determine the nature of the problem and an estimate of the restoration of services. If the vendor cannot be reached and services cannot be restored, Jon Werner will put together a team of employees from the critical service area affected to determine an appropriate “work-around” solution. may also consider referencing the vendor’s own recovery plan on file in the Chief Compliance Officer’s office to attempt to determine likely causes of the disruption and the vendor’s own estimate of the restoration of services therefrom. If continued efforts to contact the vendor and/or to restore services are unsuccessful, consider contacting a back-up or replacement vendor.

1. ALTERNATE SITE FOR BUSINESS OPERATIONS:

If ’s principal office, located at , is damaged or otherwise inaccessible, has designated Jon Werner’s residence as a temporary alternate location from which to restore normal business operations. If the expected duration of the disruption or inaccessibility of ’s principal office is longer than a month, Jon Werner will determine a more permanent alternative location or new principal office. Depending on an employee’s job requirements and the availability of a personal computer and Internet access at home, some employees may be permitted or required to work remotely for a time from his/her residence. Due to’s relatively small size and staff, this determination will be made and communicated to each employee at the appropriate time based on the particular circumstances.

Jon Werner’s residence is:

**552 Country Club Parkway SE**

**Cedar Rapids, IA 52403**

Directions to Jon Werner’s residence are as follows:

**Directions from Primary Location:**

**Going NW on 5th Avenue towards 3rd Street SE:**

* Take left onto 2nd Street
* Turn right onto 1st Avenue
* Turn right onto 27th St Dr
* Turn right onto Country Club Pkwy

In the initial stages of a disruption, each employee will be contacted and given instructions. (See Section IX “COMMUNICATIONS” of this Plan).

VII. DATA PROTECTION, BACK-UP & RECOVERY:

1. **Back Up Procedures:**

All data on systems is backed-up by **REDTAIL TECHNOLOGY** to a remote location on a daily basis. (See “VENDOR CONTACT SHEET” attached hereto as **Appendix C** for contact information). This process is fully automated and is completed via a secure Internet connection. In addition, electronically stored data is backed-up at least weekly and securely stored off-site or on the cloud is currently in the process of having files, otherwise maintained by in paper form (i.e., client agreements), scanned and disks stored offsite or on the cloud. All paper files maintained at’s principal office are kept in secure, fire-resistant filing cabinets.

1. **Recovery Procedures:**

If ’s systems are accessible and otherwise undamaged following an emergency, as may be the case in the event of a power failure, it may be possible to safely retrieve and transport ’s server and hardware systems, containing all electronically-stored data, to the alternate site for restoration of business operations. In the initial stages of the disruption, Jon Werner will make the determination regarding the physical and economic possibility and practicality of this course of action or whether a complete backup to the alternate system is warranted.

1. FROM DISASTER TO RECOVERY- A TIMELINE OF TASKS:

As we all know, disasters or traumatic events can be disorienting. Be calm. The timeline provides step-by-step guidelines for’s response and recovery from such an event. Of course, an actual emergency may require some deviation from this guide and unique situations may require creative solutions. Throughout any emergency and business disruption, we remind each employee to be mindful of’s fiduciary duty to its clients both when evaluating the situation and when determining the appropriate course of action.

See “FROM DISASTER TO RECOVERY A TIMELINE OF TASKS” attached hereto as **Appendix B**.

1. COMMUNICATIONS:
	1. **Telecommunications Disruption:**

In the event that local “land-line” telephone service is disrupted, employees are encouraged to use their personal cellular phones to conduct business until service is restored. has arranged with its local telephone service provider to use a feature called Remote Call Forwarding in the event of a local telecommunications disruption. This feature will forward all in-coming telephone calls made to the principal office to Jon Werner’s cellular telephone number. This contingency is for disruptions lasting more than a day because the forwarding system will typically be operational within 24 hours following a disruption. Using the Telephone User Guide we can initiate call forwarding or we can reach Iowa Solutions to assist having calls directed to Jon’s cell phone. Currently we are using ImOn for telephone services and our phone system is through Iowa Solutions.

* 1. **Internet & Email Service Disruption:**

Company emails are currently backed up using Smarsh/Intermedia services and Archiving through RIA in a Box (Comply). Our domain is stonefield.us and that domain is registered to Jon Werner. All emails are accessible via Smarsh’s secure online web-based portal.

LOSS OF KEY PERSONNEL:

Currently, Jon Werner is the Managing Member of all client investment accounts. Should something happen to

Jon Werner rendering him incapable of fulfilling his duties, clients could suffer lost investment opportunities, inaccessibility to accounts, etc. In such case:

1. Rebecca Hanson will notify all current clients immediately via regular mail and phone while documenting who has been reached. …
2. For successor ownership please contact Arenson Law Group, specifically Jim Arenson at (319) 363-8199

XI. TRAINING, TESTING & REVISION OF PLAN:

1. **Distribution of the Plan:**

Each employee will receive two (2) copies of the Plan and will be required to sign an acknowledgement that he/she has read and understands the Plan. (See “ACKNOWLEDGEMENT FORM” attached hereto as **Appendix G**). One copy of the Plan is to be kept at the employee’s workstation. The other copy is to be kept at the employee’s home address. ALL EMPLOYEES ARE REQUIRED TO MAINTAIN A CURRENT COPY OF THIS PLAN AT HIS OR HER HOME ADDRESS. The acknowledgement is to be provided to employees in a timely fashion. (Please note, to protect the privacy of non-public client information, not all employees’ copies of the Plan will include a Client Contact Sheet).

A copy of the Plan is also maintained in a secure location at Jon Werner’s residence

along with all relevant insurance policies. These copies will contain the Client Contact Sheet, which will be updated periodically.

1. **Training**

The Plan will be reviewed at least annually with all employees at a firm-wide meeting. Minutes of these meetings will be kept and attendance by all employees is mandatory. If an employee has any questions regarding the Plan or his/her role in the event of an emergency, he/she is encouraged to ask Jon Werner for clarification. It is imperative that all personnel are familiar with the policies and procedures of the Plan and have a thorough understanding of his/her responsibilities in the event of an emergency.

1. **Testing, Plan Revision & Recordkeeping:**

Jon Werner periodically, and on at least an annual basis, will test the Plan. Such tests may be as complex as running a simulation of an actual disaster, including the restoration of data to alternate systems, or as basic as testing the employee call tree. Typically, but not always, testing will be conducted after hours to minimize disruption of normal business operations. In order to gain realistic results that may be used to revise and optimize the effectiveness of the Plan in the event of a real emergency, not all tests will be announced ahead of time to all employees.

Test results will be evaluated and documented by Jon Werner and a determination of any weaknesses exposed by the test will be made at that time. The Plan will be revised accordingly to fill gaps discovered during testing. The Plan may also be revised pursuant to reviews and the issuance of regulatory guidance.

Changes in business operations, contracts and contacts, including new employees, new vendors or new addresses for existing employees or vendors, etc. must be reflected in the Plan. Most importantly, current client contact information must be maintained as part of the Plan. Jon Werner will be responsible for ensuring that the Plan is updated periodically and as required by the frequency of such changes. Changing the date in the lower left-hand corner of the Plan will indicate any such revision. Any revision to the Plan will be distributed to all employees and each employee will be required to provide a new, signed acknowledgement form of receipt to Jon Werner. Old copies of the Plan will be exchanged for the new copies to assure that no employee holds an out-dated copy or confuses an out-dated copy for a current copy during an emergency. A revised copy will also be placed in the safe deposit box. All prior versions of the Plan will be destroyed except for one copy maintained in ’s files as required by applicable regulations.

1. ACCESS TO FUNDS AND SECURITIES:

Our firm does maintain custody of customers’ funds or securities. In the event of a significant business disruption, we will make these funds available to our customers.

1. FINANCIAL AND OPERATIONAL ASSETS:

When a significant business disruption occurs, our Disaster Recovery Team will determine the best way for us to communicate with our employees, clients, banks, vendors, regulators, etc. The communications options we use will depend on the disruption, but may include our website, telephone, email, etc.

Our Finance Team will perform a valuation on our assets and evaluate whether we may continue our operations and remain in capital compliance. We will contact Charles Schwab and Bankers Trust to report our current financial status. In any case where we are not able to meet our obligations or fund our operations, we will seek additional financing from our bank or other credit sources. If we are unable to obtain funding, we will inform our regulators and immediately take appropriate steps, including [insert procedures].

1. MISSION CRITICAL SYSTEMS:

Our firm’s mission critical systems include:

* CHARLES SCHWAB – Custodian
* TIAA - Custodian
1. CRITICAL BUSINESS CONSTITUENTS, BANKS, AND COUNTERPARTIES:

During this business disruption, we have determined that we can continue our business relationship with our critical business constituents. If a business relationship is no longer possible, we will find alternative arrangements. Our major suppliers are:

* SMARSH/INTERMEDIA: Email and Encryption (866) 762-7741
* REDTAIL TECHNOLOGY: CRM and File Storage (800) 206-5030
* METRO STUDIOS: Website (319) 363-2002
* COMPLY (RIA in a Box): Compliance Consulting (646) 742-5391
*

The bank maintaining our operating account is: BANKERS TRUST (Sarah Netolicky) 201 1st Street SE Ste 1110 Cedar Rapids, IA 52401 (319) 896-7777. If our banks and other lenders are unable to provide the financing, we will seek alternative financing immediately from Grinnell State Bank (Jeremy Provin) 1101 Court Ave Marengo, IA 52301 (319) 642-5511.

If our transactions cannot be completed with our critical counterparties, we will contact those counterparties directly to make alternative arrangements to complete those transactions as soon as possible.

1. REGULATORY REPORTING:

Our firm is subject to regulation by the Iowa Insurance Division and the Securities and Exchange Commission (SEC). During normal business operations, we file reports through mail, fax, email, a web portals, online. If a disruption causes our firm to be unable to file normally, we will get in touch with the regulator and determine an alternative way to file that is acceptable.

1. SENIOR MANAGER APPROVAL:

I have approved this Business Continuity Plan as reasonably designed to enable our firm to meet its obligations to customers in the event of a significant business disruption.

Owner Name: JON WERNER

Owner Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**APPENDIX A**

**EMPLOYEE CONTACT SHEET**

**Jon Werner – President**

**Home Address: 552 Country Club Pkwy SE Cedar Rapids, IA 52403**

**Home Email:** **jon01werner@gmail.com**

**Cell Phone: (319) 270-3462**

**Rebecca Hanson – Office Manager**

**Home Address: 213 5th Street NW Mount Vernon, IA 52314**

**Home Email: fortab2012@gmail.com**

**Cell Phone: (319) 640-9665**

**APPENDIX B**

**FROM DISASTER TO RECOVERY**

**A timeline of tasks**

**0-2 hours**

Discovery and Assessment:

* Does disaster occur during business hours? If yes, CALL 911
	+ Is evacuation necessary? Does remaining in the bldg pose a threat to the safety of employees? If yes, evacuate building and meet safe, designated location outside of the building (Always follow Instructions of emergency personnel).
	+ If safety permits, secure all confidential client information prior to evacuation.
	+ Conduct a roll call at designated location to ensure the health and safety of all employees.
	+ Attempt to assess estimated amount of time before possible resumption. If more than one day, determine whether or not to initiate an alternative site.
* If safety does not demand evacuation of building, can normal operations resume (i.e., is there a power outage or other resulting disruption that does not permit resumption of business).
	+ If less than a day, determine whether or not to dismiss employees for a number of hours
	+ If more than a day, determine whether or not to continue work from an alternative location.
	+ If disruption results from an emergency at a key third party vendor, assess amount of time until restoration by vendor, come up with a work around or determine alternative vendor to fill the gap.
* If no, anyone initially discovering situation must notify Jon Werner immediately. Does situation preclude safe, normal business operations? (Jon Werner will make that determination).
	+ If yes, execute call tree. Inform employees of situation, direct them to avoid principal office and wait for further instructions.
	+ If no, attempt to quickly assess estimated amount of time before possible resumption and execute call tree to inform employees of situation and where and when to reconvene.

**2-6 hours**

Initiate Emergency Recovery/Contact Critical Vendors:

* Assess which staff will meet at alternative location and which will work from home. Set a time the following day for a conference call, if possible, or otherwise require each staff member to call in a set time. Notify Jon Werner accordingly.
* Begin to compile list of data lost or otherwise inaccessible.
* If possible, begin to salvage data and files from principal office or make plans for such salvage as soon as safety and the authorities permit it.
* If necessary, initiate recovery of backed up data to alternate systems.
* Begin to capture expenses associated with disruption.
* If necessary, notify insurance carriers of situation.
* Arrange with authorities and/or landlord to participate in salvage operations and secure confidential information ASAP.
* Notify and brief key vendors on situation, including broker dealers.
* Request broker dealers send (fax email or other remaining means) information regarding client holdings and trade blotters.
* Contact Telephone Company to redirect all calls made to firm to Jon Werner’s cell phone number.
* Determine if and what client communication is necessary.
* If possible and if estimated time of disruption calls for it, consider recording emergency voicemail to provide basic information regarding situation of clients and vendors calling in.
* If possible and if estimated time of disruption calls for it, contact web-host to post a notice to clients on the firm’s homepage informing them of the situation and how to contact us and any prudential information.
* If possible and if estimated time of disruption calls for it, consider sending an email to all clients informing them of situation and other important information. If disruption includes a failure of website and email systems backup national email system and send an email to all clients informing them of the situation.
* Verify that restoration of backup data was successful and systems are fully operational. If necessary, contact IT vendors for priority assistance. (If disruption is not localized, priority assistance may not be feasible, thus, testing systems before an emergency occurs is critical).

**6-8 hours**

Restoration of Normal Business Operations

* Conduct a reconciliation of accounts to verify that holdings match broker dealer information
* Resume normal operations.
* Assess damage and estimated time until principal office will be accessible and operational. If estimate is more than a month, begin to formulate plan for new principal office or more permanent alternative location.
* Review compliance checklist to determine whether any critical filings are required in the near future.
* Notify regulators to inform them of situation and new operating location, if necessary.

**APPENDIX C**

**CRITICAL VENDOR CONTACT SHEET**

**Securities and Exchange Commission:**

(800) 732-0330

**Local Phone Company:**

ImOn Communications – (319) 298-6484

**Data Backup and Recovery:**

Redtail Technology – (800) 206-5030

**Broker Dealer:**

Charles Schwab – (800) 435-4000

**Website Hosting:**

Metro Studios – (319) 363-2002

**Domain Registration:**

Metro Studios – (319) 363-2002 & GoDaddy (480) 366-3549

**Insurance Carriers:**

State Farm – (800) 782-8332

**Payroll and Accounting:**

St. John & Gielau LLP - Ron Gielau – (319) 373-9300

**Email and Encryption:**

Smarsh and Intermedia – (866) 762-7741

**Compliance and Archiving:**

Comply/RIA in a Box – (866) 611-7638

**APPENDIX D**

**BUILDING EVACUATION PLAN**

Any staff member may order an evacuation based on their assessment of potential threats

Secure the door of your office as you leave.

Use enclosed stairwell for evacuation.

* Stairwells are located in the SE and NW halls on the 12th floor. Elevators are deactivated in an emergency.

Listen for and obey instructions from safety personnel coming up the stairs.

Once out of the building, keep moving away from the building to the perimeter of the building site. Proceed directly to the primary assembly area.

* Jon Werner or Rebecca Hanson is responsible for verifying everyone is present and safe, please check in with one of them once you are in assembly area.
* Once you have left your area, do not return for personal belongings.
* Do not return to the office until the “all clear” is given to you by Jon or Rebecca.

External Assembly Area – In the event the building is evacuated proceed directly to our primary designated assembly area.

* EXTERNAL ASSEMBLY AREA: Jon Werner’s Home Address.

**APPENDIX E**

**CLIENT CONTACT SHEET**

Client Contact Sheet can be found in Redtail Imaging.

**APPENDIX F**

**TYPES OF DISASTERS – VUNERABILITY ASSESSSMENT**

 **BUISNESS IMPACT ANALYSIS**

FIRM VULNERABILITY WORKSHEET

The following is designed to assist the Disaster Recovery Team to assess the firms vulnerability and plan for possible disaster scenarios

|  |  |  |
| --- | --- | --- |
|  |  | **Approximate Risk Level** |
| 1. Is the firm located in an area at all susceptible to hurricanes, tornadoes or severe weather? | X Yes \_\_\_ No | \_\_\_ High \_\_\_ Med X Low |
| 2. Is the firm located near the shore, a flood plain or low lying area? | \_\_\_ Yes X No | \_\_\_ High \_\_\_ Med X Low |
| 3. Is the firm located in an earthquake zone or an area susceptible to volcanic activity? | \_\_\_ Yes X No | \_\_\_ High \_\_\_ Med X Low |
| 4. Is the firm located near hazardous industry or potential terrorist targets? | \_\_\_ Yes X No | \_\_\_ High \_\_\_ Med X Low |
| 5. Is the firm located in an area that may be impacted by mudslides or wildfires?  | \_\_\_ Yes X No | \_\_\_ High \_\_\_ Med X Low |
|  | \_\_\_ Yes \_\_\_ No | \_\_\_ High \_\_\_ Med \_\_\_ Low |

\*For this assessment, the following definitions of the measures of risk are used:

High – Event likely to be experienced once per year:

Med – Eventually to be experienced once every ten years.

Low – Event likely to be experienced once every hundred years.

EXPLANATION OF RESPONSES AND/OR OTHER RISKS AND COMMENTS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The following is designed to assist the Disaster Recovery Team to assess the firm

’

s vulnerability and plan for possible disaster

scenarios.

\*For this assessment, the following definitions of the measures of risk are used:

High

-

Event likely to be experienced once per year.

Med

-

Event likely to be experienced once every ten years.

Low

-

Event likely to be experienced once every hundred years.

EXPLANATION OF RESPONSES AND/OR OTHER RISKS AND COMMENTS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The above vulnerability/risk assessment is based on the firm

’

s geographic location and an attempt to account for unforeseen events.

Bear in mind that even if the firm is not currently situated in a risk

-

prone environment, critical vendors, communication lines and

transportation routes of employees may be. This is considered in the

“

Resulting Business Disruptions

”

analyisis below.

**Resulting Business Disruptions Possible**

Certain disruptions may result from any or several of the causes listed above (although the particular cause may impact the duration

of the disruption). The Plan must provide for the recovery of critical processes from these disruptions. These include (among

**Approximate Risk**

**Level\***

(

If yes, assign likelihood of

occurrence impacting firm)

1

. Is the firm located in an area at all

susceptible to hurricanes, tornados or other

severe weather?

\_\_\_ Yes \_\_\_ No

\_\_\_High \_\_\_Med

\_\_\_Low

. Is the firm located near the shore, a flood

2

plain or low lying area?

\_\_\_ Yes \_\_\_ No

\_\_\_High \_\_\_Med

\_\_\_Low

3

. Is the firm located in an earthquake zone or

an area susceptible to volcanic activity?

\_\_\_ Yes \_\_\_ No

\_\_\_High \_\_\_Med

\_\_\_Low

. Is the firm located near hazardous industry

4

or potential terrorist targets (concentrated

financial district, airport, nuclear power plant,

oil refinery, etc.)?

\_\_\_ Yes \_\_\_ No

\_\_\_High \_\_\_Med

\_\_\_Low

. Is the firm located in an area that may be

5

impacted by mudslides or wildfires?

\_\_\_ Yes \_\_\_ No

\_\_\_High \_\_\_Med

\_\_\_Low

6

.

…

\_\_\_

Yes \_\_\_ No

\_\_\_High \_\_\_Med

\_\_\_Low





\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name of Employee

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date