Business Continuity and
Disaster Recovery and Contingency Plan

Life Story Financial has created a Disaster Recovery and Contingency Plan to effectively address and state the specific steps which we shall use and employ to recover from any disaster or emergency.

Our first line of defense is the full complement of insurance that we carry. This has been tailored to protect us from a loss of financial resources in the event of a disaster. It is our understanding that acts of war are probably not covered under this or any policy.

I. Offices

Our physical location could become unusable for many reasons. Regardless of the cause, the impact would be the same, but the duration could be longer. This section focuses on the variety of scenarios we can envision and our responses to them.

A. *Short-term disruptions that cause our building to be unavailable for time frames of less than one month, such as, power outages, broken HVAC, weather emergencies, or evacuations.*

   To deal with this we would operate at a remote location, possibly out of our homes, a suite in another professional's office, or a suite/ballroom at a local hotel. Employees are to check in with management via their home phone number or cell phone number to be informed of the place of operation. Vital equipment will be transported to the site if possible or borrowed or leased at the location of operation. If needed, data will be restored from one of many different forms of data backups we have in place. Phones are to be forwarded.

B. *Intermediate-term disruptions that cause our building to be unavailable for a time frame of more than a month but less than a year, such as,* fire, contamination, flood damage, or building structural problems.

If we do not know the magnitude at the time of the event, we will utilize plan A, above until the time frame will exceed one month. We will lease temporary space from a business associate or through a commercial realtor. All equipment and files will be moved or replaced, and phone lines will be transferred to the new location. Once our building is available everything will be moved back.

C. *Permanent loss of use of the building, such as* fire, flood, or terrorist attack.

At the time of the event, we should know the severity of the event and would go right to plan B and find new permanent office space.

If the city is destroyed or rendered uninhabitable, management will choose evacuation locations. At that time, we would regroup and choose an area in our state to house our operations. We have created procedures to protect our asset management data, financial data, and other important documents. However, some less important data would have to be reconstructed. Our greatest challenge would be in contacting our clients. We would utilize whatever means necessary to do this.

II. Equipment

Our equipment needs are not very sophisticated or extensive. We utilize a Macbook Air with an Apple M1 chip with 16 GB of memory and the most recent version of the macOS. The computer's startup disk is secured with FileVault, which has built-in encryption capability to secure all data.

This setup could be operational within hours and completely restored in less than a day. Any IT specialist could do this if our current person is unavailable.

Our phone system is a voice over Internet protocol (VoIP) service that can be used in any location with an Internet connection. The rest of our office equipment is generic and can be readily replaced.

III. Regulatory Issues

We would make every effort to remain in compliance in the event of a disaster. We have transferred required paperwork to a digital format that is backed up to a portable hard drive which is taken off-site. We will be working to place a substantial portion of the other paper documents that we utilized in this format also. We would refer to the contacts listed in our Critical Contact List (attached below) as necessary in the event of a disaster to ensure that we remain in compliance.

IV. Third-Party Vendors

We do not utilize any third-party vendors that are so unique that they could not be replaced with a competitor. The only quasi-third parties that would cause us great disruption are companies that make up the infrastructure of the country. If the banking system, mail system, communication networks, security markets or federal government were rendered inoperative for any great length of time we would not be able to operate. We do not have the size or resources to provide these services ourselves.

V. Systems and Information

A. Computer systems at Life Story Financial are relatively unsophisticated in design and setup but are vital to our operation. The actual equipment is easily replaced as mentioned above. The data is almost irreplaceable, so we have implemented the following backup procedures:

    1. We store files using Google Drive, which offers cloud-based storage that is backed up as soon as changes are made to files and there is an Internet connection. We also retain and hold files in Google Vault for the purposes of information governance and eDiscovery.

B. The software that is utilized by Life Story Financial is mainstream and not customized for our operations.
    1. We use Microsoft products and Quickbooks for our business operations. Business data is stored in their cloud-based storage systems.
    2. We utilize AssetMark Trust's web-based eWealthManager software for our asset management tasks. In the event of a disaster, we could download new software for our asset management tasks. If for some reason either company ceases to exist in any form, there are other asset management software providers that we could use.
    3. We utilize Holistiplan's web-based tax planning software for our tax planning tasks. All documents uploaded to the application are encrypted with 256-TLS.
    4. We utilize Envestnet MoneyGuide's web-based financial planning software for our financial planning tasks, which is built with 256-bit encrypted SSL. It is a SOC 2, type 2-certified organization.
    5. We utilize Wealthbox's web-based software for customer relationship management, which is built with 256-bit encrypted SSL and advanced security safeguards. It is a SOC 2, type 2-certified organization.

C. Paper files are a weak link since they consume large amounts of space and are not easily transported. That is why all data is stored electronically, and the overwhelming majority of the firm's files could be recreated.

VI. Employees

Our employees are one of our most valuable resources. We make every effort to protect them from harm at the workplace and to retain them. In the event of a disaster, the staff is informed to check in with the firm owner to receive instructions. We would hire carefully screened temps and subcontract out non-confidential work in the event of a loss of employees. Life Story Financial is in the process of creating plans for ownership transfer in the event of the owner's death. If this plan is not implemented, it will be the responsibility of that person to sell the business.

This disaster/contingency plan is to be reviewed at least annually. Changes to be implemented more frequently if needed.

VII. Critical Contact List

1. **AssetMark Trust** eservice@assetmark.com, 800-664-5345
2. **Holistiplan** support@holistiplan.com
3. **Envestnet MoneyGuide** support@moneyguide.com, 800-743-7092
4. **Wealthbox** support@wealthbox.com