Disaster Recovery and Contingency Plan of LongView Wealth Management
Summary Disclosure Statement

LongView Wealth Management (LongView) has devised the within Disaster Recovery and Contingency Plan in order to effectively address and state the specific steps which we shall use and employ in order to recover from any disaster or emergency.
Our first line of defense is the full compliment 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. The following is a list of possible causes: 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 place of operation. Vital equipment will be transported to 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 and less that a year. The following is a list of possible causes: 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 it is clear that 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 back online everything will be moved back.
C.Permanent loss of use of building. The following is a list of possible causes: 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 has chosen two 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 finding the location of our clients. We would utilize whatever means necessary to do this.

II.Equipment

Our equipment needs are not very sophisticated or extensive. [Example: We utilize several standalone computers (as well as a few laptop computers), connected to Windows 2008 R2 servers. Local servers are backed using cloud based technology. The cloud drive infrastructure is a redundant set of data centers across three geographically different locations. This setup means that we can access our data from any computer at any location that has an internet access.

Our phone system is relatively simplistic and could be moved or replaced within hours and our phones can be forwarded in a fraction of that time. 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 much of the required paperwork to a digital format that is backed up and off site. We will be working to place a substantial portion of the other paper documents that we utilized in this format also. We are always in contact with our compliance attorney who is on retainer for compliance issues. She would be one of the first people we would contact in the event of a disaster to ensure that we remain in compliance and would follow her directions.

IV. Third Party

We do not utilize any third party venders 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 LongView 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. Local servers are backed up using a cloud based technology so that individual files and folders can be restored. LongView's mail server and accompanying domain controllers are hosted in a datacenter with redundant power and internet connections. The mail server and domain controllers are backed up using cloud based backup. In the event of catastrophic failure, new hardware will be purchased to replace the servers, and the data, including system state, can be restored via the cloud backups.
2. Desktop computers can be replaced in the event of disaster. Software that comes directly with new machines (OEM copies of MS Office, etc) will be re-purchased when the replacement machines are purchased. Users are storing their data on Cloud Drives.
3. As the Exchange server and Cloud Drives are externally hosted solutions, if the corporate office suffers a disaster, users will still be able to access email and data from remote locations: WiFi hotspots, home office, etc.

B. Our paper files are our weakest link, since they consume large amounts of space. They are not easily transported. We are working on the conversion of the important documents to a digital format. This process is time consuming and will be an ongoing project until all communications are done electronically. Until this time, we will make every effort to protect these files from being damaged or stolen. It is encouraging that the large 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 one of the managers to receive instructions. We would hire carefully screened temps and subcontract out non-confidential work in the event of loss of large number of employees. Any management team member could be replaced by hiring a combination of consultants and other professionals. LongView has plans for ownership transfer in the event of the owner's death. If this plan is not implemented it is the responsibility of the management team to sell the business.

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

NAME	**Cell / Home**
Bigler, Wes	678-296-4871
Bolton, Cathy	770-639-2666

Bolton, Jim	770-781-4206
Bosley, Tom	770-973-3748
Diaz, Hector	404-502-2710 / 770-467-9873
Dwyer, Kris	678-488-6501
Ellis, Bruce	404-388-8309
Fisher, Quinton	404-281-9481
Ganser, Susan	404-245-2027
Lancaster, Joey	770-616-3035
Licata, Kirk	908-370-9464
Lipsey, Michael	404-234-1984
McKay, Mike	404-387-8289 / 706-568-0662
Nicastro, Carmen	770-713-4160 / 770-579-8755
Stefanini, Doug	678-592-8067 / 404-748-1903