Toolkit Template
Business Continuity and Disaster Recovery Plan

Objective: This template has been developed to document critical activities and information related to your business in the event of the incapacitation of your executive leader or owner. This toolkit profiles strategies and provides a guide for responding to a physical disaster (weather, fire, earthquake, flood, etc.) or a cyber disaster, such as a data breach.

With the GIS BG&C portal, there are multiple areas that you can access to guide you through the creation of a Disaster Recovery Plan. The following includes high-level prompts to ensure that your firm has taken the necessary steps to recover from a physical or cyber disaster.

Prior to the event of a physical disaster, the following activities should be completed to create a disaster recovery plan;

- Has your firm developed a disaster recovery plan?
- Has this plan been tested?
- Has this plan been tested over the last six months?
- Have you reviewed the plan for gaps and omissions as your firm has grown or changed over the last six months?
- Have you amended the plan to fill these possible gaps and omissions?
- Are executives or key staff aware that a disaster recovery plan exists and how they are to follow the plan in the case of a physical disaster?

With the increasing threat of data breach, ransom ware and other IT outages, your disaster plan should include responses for a myriad of events, including:

- Data Breach
  - Have you developed an incident response plan in the event of a data breach?
  - Have you had a cyber audit performed on your network and systems?
  - Are you running anti-malware software on all enterprise devices, and is it up to date?
  - Have you contracted with a service to support the physical and forensic response to a breach and make certain that your firm is in compliance with all reporting and communication regulations?

- System failure
  - Have you performed a system failure test in the last six months?
  - Have you modified your plan to reflect changes to your software and hardware?

- Communications network outage
  - Have you performed a communications network outage test in the last six months?
  - Have you modified your plan to reflect changes to your software and hardware?

- Provider outage
  - In the event of a provider outage, do you have recent backups of all critical programs and data related to that provider?
  - Do you have a list of alternate providers, if needed?