Disaster response policy for a single person registered investment advisors' office

Policy Purpose and Scope

This Disaster Response and Business Continuity Policy (“Policy”) describes how the Firm will prepare for, respond to, and recover from events that disrupt normal operations, including natural disasters, technology failures, and other emergencies that could impact client service or the integrity of books and records.[1][2]

This Policy applies to all advisory activities conducted by the Firm’s sole owner and investment adviser representative (“IAR”), including operations conducted at the primary office, any home office, and when working remotely.[2]

Objectives

The objectives of this Policy are to:

- Protect the safety of the Firm’s personnel (the sole proprietor) and, where applicable, visitors.
- Maintain the integrity and availability of client accounts, books, and records.
- Provide for timely communication with clients, custodians, vendors, and regulators.
- Resume critical advisory operations as quickly and safely as possible following a disruption.[1][2]

Risk Assessment and Key Scenarios

The Firm has considered the following reasonably foreseeable events:

- Physical office disruptions: fire, flood, severe weather, utility outage, or loss of access to the office.
- Technology disruptions: internet or power outage, hardware failure, cyber incident, or loss of primary systems.
- Regional events: natural disasters or community-wide emergencies impacting a broad geographic area.
- Personal events: disability or death of the Firm’s sole owner that prevent continuation of services.[3][2]

The Firm will review this risk assessment at least annually and update it as necessary.[3][2]

Critical Functions

The Firm has identified the following critical functions that must be restored first after a disruption:

- Ability to monitor client portfolios and markets via custodian and trading platforms.
- Ability to enter trades or instruct the custodian when necessary to protect clients.
- Access to client information, portfolio data, and compliance records.
- Ability to communicate with clients, custodians, vendors, insurers, and regulators.[2]

Where possible, the Firm maintains redundancy and remote access for these functions (e.g., cloud-based systems and secure remote logins).[4][2]

Books, Records, and Data Backup

- The Firm maintains required books and records in electronic form using secure, password-protected systems, including portfolio management/compliance tools and cloud storage.
- Critical records (e.g., client agreements, Form ADV, policies and procedures, financial records) are backed up regularly and stored in at least one off-site or cloud location separate from the primary office.[5][4]
- The Firm tests access to backup systems at least annually to confirm data can be restored in the event of a disruption.[5][2]

Immediate Response to an Event

When a disruption occurs, the Firm will follow these steps, in order of priority:

1. **Personal safety**
   - Evacuate the premises if necessary and contact emergency services (911) as appropriate.[4][5]
   - Follow local emergency guidance for shelter-in-place or evacuation orders.[1]
2. **Stabilize operations**
   - Determine the nature and expected duration of the disruption (e.g., brief outage versus extended loss of facilities).[2]
   - If safe, secure physical files, equipment, and devices to prevent further loss or damage.[4][5]

3. **Activate alternate operations**
    - If the primary office is unavailable or unsafe, operate from a designated alternate location (e.g., home office or other remote workspace) using laptop and cloud-based systems.[4][2]
    - Utilize backup internet or connectivity options (e.g., hotspot, secondary ISP) to access custodian and vendor systems.[4]

Communication Plan

In the event of a significant business disruption, the Firm will use the following communication framework:

- **Clients**
    - As soon as practical (typically within one to two business days), the Firm will notify clients of:
        - The nature of the disruption.
        - Any expected impact on services.
        - How to contact the Firm and/or directly contact their custodian.
    - Communication methods may include email, phone, website updates, or secure client portals, depending on what systems are available.[5][2][4]
- **Custodians and key vendors**
    - The Firm will promptly notify custodians and essential vendors (e.g., technology providers, compliance vendors) of any disruption that may affect trading, reporting, or access to systems.[2]
    - The Firm will confirm their business continuity readiness and any special procedures they have activated.[2][4]
- **Regulators**
    - If required by applicable law or regulation (e.g., in the event of a material disruption or cybersecurity incident impacting clients), the Firm will notify the appropriate regulator(s) and follow their guidance.[6][2]

Key contact information (clients, custodians, vendors, regulators, insurance, and emergency services) is maintained in both electronic and printed form and is accessible from alternate locations.[5][4]

Alternative Office and Remote Work

- The Firm's primary alternative office is the adviser's home office or other secure remote location equipped with necessary technology (computer, phone, internet).[4][2]
- The Firm's systems (custodian portals, portfolio management, email, and document storage) are accessible through secure remote connections using multi-factor authentication.[4]
- Hardware and software needs (e.g., replacement laptops or peripherals) will be sourced as quickly as possible if primary equipment is damaged.[2]

Trading, Portfolio Monitoring, and Client Instructions

- The Firm monitors client portfolios and markets using custodian and portfolio management platforms that can be accessed from alternate locations.[2]
- In the event of a disruption affecting normal trading channels, the Firm will coordinate with the custodian to implement any necessary trades or protective measures using alternative procedures (e.g., phone-based trading procedures where available).[2]
- If the Firm is temporarily unable to access systems, clients will be directed to contact their custodians directly for urgent account-level needs.[4][2]

Financial Resilience and Insurance

- The Firm maintains appropriate insurance (e.g., property, liability, and business coverage) and will promptly file claims in the event of a covered loss.[7][5]
- The Firm maintains an emergency cash reserve or credit access sufficient to cover essential business expenses during a temporary interruption.[7][4]
- The Firm periodically reviews coverage and financial preparedness to ensure it remains adequate in light of current operations and risks.[7][5]

Cybersecurity and Data Protection During a Disaster

- During and after a disruption, the Firm will continue to follow its cybersecurity controls, including the use of secure networks, encryption where applicable, and multi-factor authentication.[4][2]

- In the event of a suspected data breach or cyber incident, the Firm will follow its separate Incident Response procedures, including notifying clients and regulators as required.[8][2]

Succession and Permanent Interruption Planning

In the event of the Firm owner's death, disability, or permanent inability to continue operations:

- The Firm's designated successor or contingency firm (if applicable) will assume responsibility for client communications and the orderly transfer or wind-down of accounts.[2]
- If the Firm will be closed:
  - Clients will be notified of the Firm's dissolution and provided with instructions for contacting custodians directly and/or selecting a new adviser.
  - Required filings (e.g., Form ADV-W for state-registered advisers) will be made to terminate registration.[6][2]
  - Books and records will be maintained for the required retention period by the designated records custodian.[6][2]

The Firm will document any succession arrangements and review them at least annually.[2]

Testing, Training, and Review

- The Firm will test key elements of this Policy (e.g., remote access, data restoration, and communication procedures) at least annually.[2]
- Following any actual disruption or test, the Firm will document performance, identify weaknesses, and update this Policy as needed.[3][2]
- Updates to this Policy will be reflected in the Firm's compliance manual and, where appropriate, summarized in Form ADV disclosures.[6][2]

Policy Maintenance

- This Policy is reviewed at least annually and upon any material change in the Firm's operations, technology, or risk profile.[3][2]
- The Firm maintains both an electronic and printed copy of this Policy, stored in locations accessible during a disruption (e.g., cloud storage and off-site physical copy).[5][2]

⁂ Additional References

1. https://www.sba.gov/business-guide/manage-your-business/prepare-emergencies
2. https://www.comply.com/resource/ria-business-continuity-and-disaster-recovery-planning/
3. https://www.cwgadvisors.com/blog/disaster-preparedness
4. https://www.blockadvisors.com/resource-center/manage-your-business/business-disaster-recovery-plan/
5. https://www.caloes.ca.gov/office-of-the-director/policy-administration/private-ngo-coordination/disaster-preparedness-for-business/
6. https://www.nasaa.org/industry-resources/investment-advisers/investment-adviser-guide/
7. https://www.ml.com/articles/steps-to-recover-financially-after-a-natural-disaster.html
8. https://www.morganlewis.com/~/media/files/publication/morgan lewis title/white paper/im--business-continuity-registered-funds-guidance-aug2016.ashx?la=en
9. https://flofr.gov/divisions-offices/division-of-securities
10. https://www.uschamberfoundation.org/solutions/disaster-response-and-resiliency
11. https://pbucc.org/images/pbucc/EY_Financial/April_19_Creating_a_Disaster_Plan_for_Your_Finances_30min_Manual.pdf
12. https://www.ssb.texas.gov/securities-professionals/dealer-adviser-registration/getting-started-registered-investment-adviser-3
13. https://kfi.ky.gov/newstatic_info.aspx?static_id=241
14. https://www.uschamber.com/security/beyond-the-payoff-how-investments-in-resilience-and-disaster-preparedness-protect-communities