

**Your Company**

# **Business Continuity Plan (BCP)**

Dated:

# Table of Contents

I.	Introduction.....	1
II.	Emergency Contact Person .....	1
III.	Branch Policy .....	1
IV.	Business Description .....	2
V.	Office Locations .....	2
VI.	Alternative Physical Location(s) of Employees .....	3
VII.	Customers' Access to Funds and Securities .....	3
VIII.	Data Back-Up and Recovery (Hard Copy and Electronic) .....	3
IX.	Financial and Operational Assessments .....	4
X.	Mission Critical Systems.....	5
XI.	Alternate Communications Between the Firm and Customers, Employees, and Regulators .....	6
XII.	Critical Business Constituents, Banks, and Counter-Parties.....	7
XIII.	Regulatory Reporting .....	9
XIV.	Disclosure of Business Continuity Plan.....	9
XV.	Updates and Annual Review .....	9
XVI.	Senior Manager Approval .....	10
	Attachment A: Damaged Books and Records Log.....	1
	Attachment B: Client Name Technology Plan .....	1
	RIA WorkSpace Technology Plan.....	1

## I. Introduction

This manual documents the business continuity plan for Client Name, LLC, a Registered Investment Advisor that conducts business in equities, fixed income securities, mutual funds, exchange traded funds, qualified plan advising, and life insurance. The purpose of this manual is to document the plans for the recovery of our critical business functions and systems in the event of a business disruption.

## II. Emergency Contact Person

Client Name provides FINRA with the contact information for 2 emergency contact persons to fulfill this requirement for all branch office locations under Client Name. These 2 emergency contact persons are registered principles for Client Name. Client Name stays in compliance by updating this information upon any material change and reviewing the information quarterly to ensure it is up to date.

Client Name, LLC has two emergency contacts as well. They are as follows:

Name 1

Name 2

*Rule: FINRA Rule 4370(f); NASD Rule 1160.*

## III. Branch Policy

Our branch's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and our property, making a financial and operational assessment, quickly recovering and resuming operations, protecting all of our branch's books and records, and allowing our customers to transact business. In the event that we determine we are unable to continue our business, we will direct our customers to the Client Name service center at (XXX) XXX-XXXX for emergency assistance and access to their funds.

### A. Significant Business Disruptions (SBDs)

Our plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only our branch's ability to communicate and do business, such as a fire in our building. External SBDs prevent the operation of the securities markets or a number of branches, such as a terrorist attack, a city flood, or a wide-scale, regional disruption. Our response to an external SBD relies more heavily on other organizations and systems, especially on the capabilities of Client Name.

### B. Approval and Execution Authority

Name 1 Chief Compliance Officer, is responsible for reviewing the plan annually.

Name 2, Managing Partner is responsible for approving the plan and has the authority to execute this BCP.

### C. Plan Location and Access

Our branch will maintain copies of this BCP plan, and the changes that have been made to it for inspection. An electronic copy of our plan is located on: xxxxxx. All employees will receive a hard copy of this document, as well as any subsequent updates, in their Compliance Binder.

*Rule: FINRA Rule 4370(b), (d) and (e).*

## IV. Business Description

Our branch office conducts business in: equity, fixed income, mutual funds, exchange traded funds, derivative securities, and life insurance products. We accept and enter orders and service retail customers and foundations/endowments. Our branch serves Qualified Plans as an advisor and does not accept or enter orders on the plan's behalf. All plans are participant directed, and are maintained by third party Administrators, Record Keepers, and Custodians that are not affiliated with Client Name, LLC

Client Name performs all clearing functions and maintains custody of retail customer funds or securities on our behalf for all discretionary assets. All transactions are sent to Client Name, which executes our orders, compares them, allocates them, clears and settles them. Client Name also maintains our customers' accounts, can grant customers access to them, and delivers funds and securities.

Client Name is located at:

City	City 2	City 3
Client Name	Client Name	Client Name
One Main Street	One Main Street	One Main Street
Anywhere, US 00000	Anywhere, US 00000	Anywhere, US 00000

Our contact number for Client Name is:

(XXX) XXX-XXXX

## V. Office Locations

Our office locations are:

### A. Office Location #1

Client Name, LLC  
One Main Street  
Anywhere, US 00000  
(XXX) XXX-XXXX

All advisory and brokerage services are performed at this location.

### B. Office Location #2

Client Name, LLC  
One Main Street  
Anywhere, US 00000  
(XXX) XXX-XXXX

This is an office on convenience for client meetings. No books & records are maintained there.

### C. Office Location #3

Client Name, LLC

One Main Street  
Anywhere, US 00000  
(XXX) XXX-XXXX

This is an office on convenience for client meetings. No books & records are maintained there

## VI. Alternative Physical Location(s) of Employees

In the event of an SBD, we will move our staff from affected office(s) to the closest of our unaffected office location(s). If none of our other office locations is available to receive those staff, we will move them to:

Client Name, LLC  
One Main Street  
Anywhere, US 00000  
(XXX) XXX-XXXX

Rule: FINRA Rule 4370(c)(6).

## VII. Customers' Access to Funds and Securities

XXXX maintains custody of customers' funds or securities on our behalf. In the event of an internal or external SBD, if telephone service is available, our registered persons will take customer orders or instructions and contact Client Name on their behalf, and update the firm phone system recorded message with situation updates. If our Web access is available, our branch will post on our website that customers may access their funds and securities by contacting Client Name at: (XXX) XXX-XXX. The website can be updated by calling XXXX at XXX-XXX-XXXX and providing them our ID # XXXX.

All Qualified Plan funds are held with third party custodians and therefore will not be affected by an internal or external SBD of Client Name, LLC. These assets are non-discretionary.

If the Securities Investor Protection Corporation (SIPC) determines that we are unable to meet our obligations to our customers or if our liabilities exceed our assets in violation of Securities Exchange Act Rule 15c3-1, SIPC may seek to appoint a trustee to disburse our assets to customers. We will assist SIPC and the trustee by providing our books and records identifying customer accounts subject to SIPC regulation.

Rules: FINRA Rule 4370(a); Securities Exchange Act Rule 15c3-1; see also 15 U.S.C. § 78eee.

## VIII. Data Back-Up and Recovery (Hard Copy and Electronic)

Our branch maintains its primary hard copy books and records at:

Client Name, LLC  
One Main Street  
Anywhere, US 00000  
(XXX) XXX-XXXX

Our branch maintains its primary electronic records on a terminal server with redundant physical locations across the United States.

Name 1, is responsible for the maintenance of these books and records. Our branch maintains the following document types and forms that are not transmitted to **Client Name**: New Account Advisory Agreements, miscellaneous working documents, outgoing/incoming correspondence, check / security receipt log, Non-cash compensation logs, Form ADV Part 2, Privacy Policy, Compliance Files, Insurance Policy Applications, RIA Policy and Procedures Manual, RIA Code of Ethics.

All working files and programs are stored in a citrix server environment, managed by RIA WorkSpace. This server can be remotely accessed using a secure log in process from any location with internet access.

See Attachment B for additional details about the **Client Name** technology plan.

Rule: *FINRA Rule 4370(c)(1).*

## IX. Financial and Operational Assessments

### A. Operational Risk

In the event of an SBD, we will immediately identify what means will permit us to communicate with our customers, employees, critical business constituents, critical banks, critical counter-parties and regulators. In addition, we will retrieve our key activity records as described in the section above, Data Back-Up and Recovery (Hard Copy and Electronic). If needed, we will direct customers directly to **Client Name** at: (XXX) XXX-XXXX. A notification will be posted to our website with instructions to clients on how to reach their advisor and to contact **Client Name** directly should they be unable to reach a **Client Name** team member.

Rules: *FINRA Rules 4370(c)(3),(c)(4), (c)(5), (c)(7), (c)(9 & (g)(2)).*

### B. Financial and Credit Risk

In the event of an SBD, we will determine the value and liquidity of our investments and other assets to evaluate our ability to continue to fund our operations and remain in capital compliance. We will contact **Client Name**, critical banks and investors to apprise them of our financial status. If we determine that we may be unable to meet our obligations to those counter-parties or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations to our customers and clients. If we cannot remedy a capital deficiency, we will file appropriate notices with our regulators and immediately take the appropriate steps.

Rules: *FINRA Rules 4370(c)(3), (c)(8) & (g)(2).*

### C. Pandemic Planning

In the event that the Managing Partner, Name 2, determines that a Pandemic event has made it impossible to operate the firm as usual, the office will be closed and business will resume with employees working remotely through the secure Terminal Server from home with their home computer and their cell phone. This will be communicated to employees through the phone tree. Employees will be required to remain home should they be affected by the Pandemic so as not to spread it to other employees and/or visitors to our office.

Information on the status of a Pandemic, and how best to prevent its spread, can be found on the following organization's websites:

World Health Organization: <http://www.who.int/en/>

Center for Disease Control: <http://www.cdc.gov/>

## X. Mission Critical Systems

“Mission critical systems” are those that ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.

We have primary responsibility for establishing and maintaining our business relationships with our customers and have sole responsibility for our mission critical functions of order taking and entry. Client Name provides the execution, comparison, clearance and settlement of securities transactions, maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.

### A. Our Branch’s Mission Critical Systems

#### **Order Taking**

Currently, we receive orders from customers via telephone, or in person. During an SBD, either internal or external, we will continue to take orders through any of these methods that are available and reliable, and in addition, as communications permit, we will inform our customers when communications become available to tell them what alternatives they have to send their orders to us. If customers are unable to reach the branch to place trades they can contact Client Name’s Service Center at (XXX) XXX-XXXX.

#### **Order Entry**

Currently, we enter orders by recording them electronically and sending them to XXXX electronically through Web Application or telephonically.

In the event of an internal SBD, we will enter and send records to XXXX by the fastest alternative means available, which include telephone or Web Application. In the event of an external SBD, we will maintain the order in electronic format, and deliver the order to XXXX by the fastest means available when it resumes operations. In addition, during an internal SBD, we may need to refer our customers to deal directly with XXXX for order entry.

#### **Order Execution**

XXXX executes orders on our behalf. Client Name’s Office 1 and Office 2 serve as primary locations for Trade Execution. Each office serves as the backup for the other. There are documented and tested plans in place to provide for a fail-over between the two sites.

#### **Other Services Currently Provided to Customers**

In addition to those services listed above in this section, we also provide insurance and qualified plan services to clients when applicable. In the event of an internal SBD, we would continue providing these services from off-site locations via phone and internet. In the event of an external SBD, we would continue providing these services via phone and internet.

## B. Mission Critical Systems Provided by Client Name

Our branch relies on Client Name to provide order execution, order comparison, order allocation, customer account maintenance and/or access and delivery of funds and securities.

Client Name backs up our records at a remote site. Client Name's Office 1 and Office 2 serve as primary locations for mission-critical processing, including: Operations, Trade Execution and Processing, and the Service Center. Each office serves as the backup for the other. There are documented and tested plans in place to provide for a fail-over between the two sites.

Rules: FINRA Rules 3510(c)(2) & (g)(1).

# XI. Alternate Communications Between the Firm and Customers, Employees, and Regulators

## A. Customers

We now communicate with our customers using the telephone, email, our website, fax, U.S. mail and in-person visits at our office or another location. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. For example, if we have communicated with a party by email but the Internet is unavailable, we will call them on the telephone and follow up where a record is needed with paper copy in the U.S. mail.

We will use whatever means of communication available to us including email, phone, our website or updating our voicemail to instruct our clients to contact the Client Name client line if we will be unable to transact business for them due to power or network outages.

Rule: FINRA Rule 4370(c)(4).

## B. Employees

We now communicate with our employees using telephone, email, and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party. We will also employ a call tree so that senior management can reach all employees quickly during an SBD. The call tree includes all staff home and office phone numbers. We have identified persons, noted below, who live near each other and may reach each other in person:



The person to invoke use of the call tree is: Name, Managing Partner

Caller	Call Recipients	Phone	Personal Email

Rule: FINRA Rule 4370(c)(5).

C. Regulators

We communicate with our regulators using telephone, email, fax, U.S. mail and in person. In the event of an SBD, we will assess which means of communication are still available to us, and use the means closest in speed and form (written or oral) to the means that we have used in the past to communicate with the other party.

Rule: FINRA Rule 4370(c)(9).

## XII. Critical Business Constituents, Banks, and Counter-Parties

A. Business constituents

Critical business constituents are businesses with which we have an ongoing commercial relationship in support of our operating activities such as vendors providing critical services.

Client Name provides most of our critical services. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of a SBD to them or our firm.

Our other critical business constituents are:

Business Constituent	Services Provided:	Phone Number	Alternatives in the event they are unavailable:
RIA WorkSpace	IT Support, Server hosting, Data back ups	773-530-1234	

Rules: FINRA Rule 4370(c)(7).

**B. Banks**

We have contacted our banks and lenders to determine if they can continue to provide the financing that we will need in light of the internal or external SBD. The bank maintaining our operating account is: Bank Name, Address, (XXX) XXX-XXXX, Bank Contact Name.

If our banks and other lenders are unable to provide the financing, we will seek alternative financing immediately from Bank Name, Address, (XXX) XXX-XXXX, Bank Contact Name.

Rules: FINRA Rule 4370(c)(7).

**C. Counter-Parties**

Client Name maintains the relationships with our critical counter-parties on our behalf. Where the transactions cannot be completed, we will work with Client Name or contact those counterparties directly to make alternative arrangements to complete those transactions as soon as possible.

Rules: FINRA Rule 4370(c)(7).

### XIII. Regulatory Reporting

We are subject to regulation by the SEC, FINRA, the Illinois Insurance Commissioner, and the Department of Labor. We now file reports with our regulators using paper copies in the U.S. mail, and electronically using fax, email and the Internet. In the event of an SBD, we will check with the SEC, FINRA and other regulators to determine which means of filing are still available to us, and use the means closest in speed and form (written or oral) to our previous filing method. In the event that we cannot contact our regulators, we will continue to file required reports using the communication means available to us.

SEC  
175 W. Jackson Boulevard  
Suite 900  
Chicago, IL 60604  
(312) 353-7390

FINRA  
(212) 858-4200

Illinois Department of Insurance  
100 W. Randolph St. Suite 9-301  
Chicago, IL 60601-3395  
(312) 814-2427

Department of Labor  
(866)487-2365

Rule: FINRA Rule 4370(c)(8).

### XIV. Disclosure of Business Continuity Plan

Client Name has a BCP disclosure statement that is provided to our customers at account opening and attached to this document as "Attachment C".

Rule: FINRA Rule 4370(e).

### XV. Updates and Annual Review

We will update this plan whenever we have a material change to our operations, structure, business or location or to those of Client Name. In addition, our firm will review this BCP annually to modify it for any changes in our operations, structure, business or location or those of Client Name.

Rule: FINRA Rule 4370(b).

## XVI. Senior Manager Approval

I have approved this Business Continuity Plan as reasonably designed to enable our branch to meet its obligations to customers in the event of an SBD.

*Rule: FINRA Rule 4370(d).*

Signed: \_\_\_\_\_

Title: \_\_\_\_\_

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

## Attachment A: Damaged Books and Records Log

### A. Finra Guidance on Books and Records Maintained at the Affected Locations

Members that maintained books and records at the affected locations should make every effort to retrieve or back-up such records. If any such records were permanently destroyed, a list of the types of books and records required to be maintained pursuant to NASD Rule 4510 and SEA Rules 17a-3 and 17a-4 must be prepared. The list should include the time periods affected, but need not include records that can be recreated from an electronic database or that can be retrieved otherwise from a service bureau, back-up records storage facility, etc. All such lists must be submitted to **Client Name** through the Compliance Service Center at 1-(800) 877-7210 x6835.

Identifiable? (Y/N)	Document Category (Finra Rule 4510, NYSE Rule 440 or SEC Rules 17a- 3 and 17a-4)	Description of records and information contained	Time Period	Backed Up/ Stored Electronically? (Y/N)	If stored offsite or electronically enter location	Can be re- created? (Y/N)

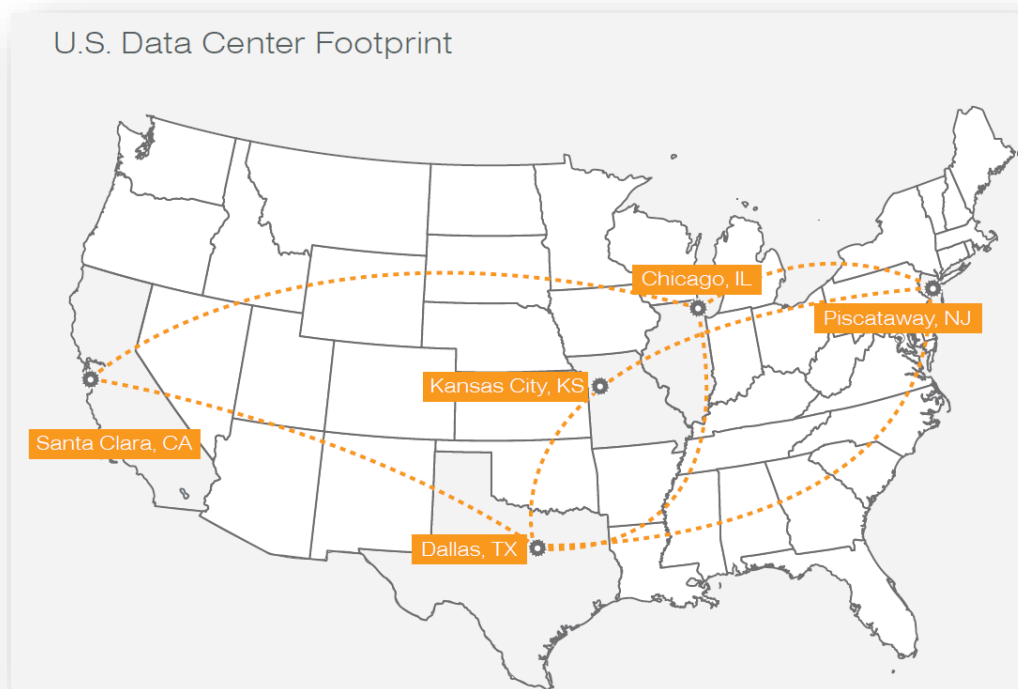

## Attachment B: Client Name Technology Plan

### RIA WorkSpace Technology Plan

#### B. RIA WorkSpace

The RIA WorkSpace Platform was designed to offer small and mid-sized financial services firm maximum flexibility without compromising security. An intuitive dashboard makes all your business files, data and applications - both windows and web-based - accessible. A secure, centralized management system works to protect your data and make it easier for your business to comply with regulatory requirements.

#### C. RIA WorkSpace Data Center Footprint



#### D. Physical Access

Access to RIA WorkSpace Data Centers is restricted to authorized personnel by security officers and two-factor authentication that includes biometric scanners. All entrances and common areas are monitored 24/7 via closed-circuit cameras, and recorded continuously. At a minimum, all our facilities must employ the following security features.

- Staffed 24/7/365 with on-site security officers
- Visitors screened upon entry, identity verified, and escorted to appropriate locations
- Doors secured using biometric hand geometry readers and pass codes
- Building exterior fully anonymous, no windows, identifying marks and is bulletproof
- All entrances protected with silent alarms and automatic notifications to authorities

- Hi-resolution digital video cameras with archiving/retrieval capabilities.

### E. Physical Structure

The building shell, exterior, floors, and roof of all RIA WorkSpace Data Center facilities meet or exceed local building codes and standards. In order to provide further protection, these facilities are built to effectively manage and withstand the effects of fire, flood and earthquakes.

### F. Fire Suppression

- A dual-alarmed, dual-interlock, multi-zoned, water-based dry pipe fire protection system ensures an ideal environment.
- Sensory mechanisms (HSSD) are utilized to sample air and sound alarms prior to water pressurization.

### G. Flood Control & Earthquake Management

- All RIA WorkSpace Data Centers are above sea level, as well as 500- year flood plains. They have no basements, have tightly sealed conduits, and moisture barriers on the exterior walls.
- Every RIA WorkSpace Data Center contains dedicated pump rooms, drainage/evacuation systems, and moisture detection sensors.
- RIA WorkSpace Data Centers are built to meet or exceed seismic design requirements of local building codes for lateral seismic design forces.

### H. Environmental Control

- In order to provide optimal environmental conditions for operation, the HVAC systems provide RIA WorkSpace Data Centers with appropriate levels of airflow, temperature, and humidity.
- The HVAC systems use N+1 redundancy configurations and are also backed up by redundant diesel generators.

### I. Redundant Power Systems

Redundant power includes uninterruptible power supplies (UPS) and backup generators, including on-site multiple-day fuel supply. Generator power is activated automatically in the event of a grid failure.

- Carrier diversity via multiple Tier 1 providers
- Redundant backup diesel generators, including on-site multiple-day fuel capacity
- Redundant 208v/30amp power to each cabinet
- N+1 HVAC
- N+1 UPS
- N+1 generators
- N+1 power distribution units (PDU)
- Full network tape backup services, offsite storage, and disaster recovery

### J. Enterprise-level Infrastructure and Backbone

- RIA WorkSpace Data Centers feature Cisco multilevel architecture with redundant fiber-optic connections from multiple Tier 1 carriers. We provision a variety of dedicated circuits, including Gigabit Ethernet (GigE).



## K. SSAE16 SOC1 Type II Certification

SSAE16 is an internationally recognized auditing standard, which gives you confidence that we follow the most rigorous standards for controls and safeguards available when hosting or processing your data.

## L. Network Security

With RIA WorkSpace, your network will have security built into the infrastructure, from end-to-end. Among other tools, we use managed Cisco firewalls, enterprise-level security appliances and intrusion prevention systems. We also backup our clients with fully redundant security appliances. In the end, if your business isn't safe, neither is ours.

## M. Intrusion Detection and Prevention Systems

RIA WorkSpace employs systems that actively monitor all network traffic to detect any attempt to log in or access resources without authorization. If suspicious activity is detected, protective measures are taken and our technicians are notified immediately.

## N. Centralized Security & Password Controls

Centralized systems make our network infrastructure easier to secure. A single point of access, connected to centralized permissions ensures that all users are properly authenticated and only have access to appropriate applications and data. Our built in password management controls further strengthen security and facilities compliance, and adhere to government regulations.

## O. End-to-End Encryption of Remote App Delivery

With our hosted application delivery, data is kept in your chosen Data Center, while only screen updates, mouse clicks, and keystrokes travel the network.

As for those things that do traverse the Internet, we provide centralized password control, multi-factor authentication, and encrypted delivery.

## P. Network Operations Center

We continuously monitor each piece of hardware and every service running within our Data Centers from the Network Operations Center 24/7/365. We make sure everything is up and running and working properly. If there's an issue, we resolve it, most of the time well before you even know about it.

Our Network Operations Center is responsible for:

- Proactive network management
- 24/7/365 monitoring of all systems
- Daily monitoring of all backups and security threats
- Deploy software upgrades and patches
- Troubleshooting and resolution
- Monthly trend and performance analysis
- Virus protection and security analysis
- Preventive maintenance to reduce network support needs

## Q. Regulatory Compliance

Every Data Center is SSAE16 SOC1 Type II compliant, meets Securities and Exchange Commission (SEC) requirements, complies with the Sarbanes-Oxley (SOX) Act, and Health Insurance Portability and Accountability Act (HIPAA) guidelines.

## R. Backups

RIA Workspace backup approach is based on Data Protection from a Recovery Point perspective. In the background, CommVault supports VM backups and iData Agent (IDA) backups, among other options. We conduct a 30-day retention, typically a weekly full synthetic backup of the VM is created on a weekend. This is the longest backup job, but consolidates a complete VM backup image. Daily incremental backups are run through the week. These backups are shorter, to minimize the overall backup window. In addition to the above weekly and daily backup, shadow copy is configured to backup every 2 hours between the hours of 7am and 9pm.