BlackBay Capital Advisors, LLC
Business Continuity/Disaster Recovery Plan

BlackBay Capital Advisors, LLC ("BlackBay" or the "Firm") maintains this Business Continuity and Disaster Recovery Plan ("BCP") to establish procedures reasonably designed to protect:

- Clients
- Personnel
- Firm operations
- Confidential information
- Technology infrastructure
- Communications systems
- Regulatory obligations

This Plan is designed to support the continuation and recovery of critical business operations during periods of disruption, emergency, cyber incident, or disaster.

The objectives of this Plan are to:

- Maintain continuity of advisory operations
- Protect client information and records
- Preserve critical communications capabilities
- Restore operational functionality as quickly as reasonably possible
- Maintain regulatory compliance
- Reduce operational risk during disruptions
- Provide guidance for personnel during emergencies

This Plan applies to:

- Employees
- Officers
- Contractors
- Supervised persons
- Remote personnel
- Cloud-based operations
- Third-party technology vendors

The Plan covers both physical and digital business disruptions.

The Firm's continuity planning addresses disruptions including but not limited to:

- Natural disasters
- Fire
- Severe weather
- Power outages
- Telecommunications failures

- Internet outages
- Cybersecurity incidents
- Ransomware attacks
- Cloud service interruptions
- Hardware failures
- Vendor disruptions
- Public health emergencies
- Office inaccessibility
- Data corruption events

The Firm has identified the following critical functions:

- Client communications
- Portfolio management
- Trading supervision
- Custodian access
- Email communications
- Regulatory communications
- Financial recordkeeping
- Cloud systems access
- Cybersecurity monitoring
- Compliance oversight

The Firm prioritizes restoration of these functions during a disruption.

Backup Facilities

In the event the Company's main office becomes unavailable to conduct operations, the Company has designated the following backup facility, located in a separate geographical location, where firm personnel can resume business activities:

Address: 1511 Locust Unit 803 St. Louis, MO 63103

Telephone: 217-257-5438

The Company Main Filing System (Junxure) is on a cloud system which can be accessed from any location in the event of an emergency. Further, Charles Schwab, Profunds, Guggenheim, and Ameritas have data storage of our client information at a backup facility if we need essential documentation. A listing of customer contact information, including names, phone numbers, and electronic mail addresses are maintained on our Cloud Junxure system. In the event the plan is updated or modified, the Company will ensure that the edited plan is distributed to key employees and that all other employees are notified of changes to the plan.

The Firm maintains the ability for authorized personnel to operate remotely using secure systems.

Remote continuity procedures may include:

- Secure remote login capabilities
- Multi-factor authentication ("MFA")
- Cloud-based file access
- Redundant communication methods
- Remote access to custodial systems
- Secure collaboration platforms

Personnel are required to follow Firm cybersecurity procedures during remote operations.

Potential incidents may include:

- Unauthorized access
- Phishing attacks
- Malware
- Ransomware
- Data breaches
- Credential compromise
- Vendor-related incidents

Incident response procedures may include:

- Access restriction
- Credential resets
- Vendor coordination
- Internal escalation
- Client notification where appropriate
- Regulatory consultation where necessary
- Restoration from backup systems

Cybersecurity Safeguards

The Firm maintains safeguards that may include:

- Multi-factor authentication
- Password controls
- Access controls
- Device security
- Anti-malware protections
- Secure cloud environments
- Encryption procedures
- Vendor security review

Personnel are expected to comply with all cybersecurity procedures.

During a disruption, the Firm will make reasonable efforts to communicate with clients through available channels including:

- Email
- Website notices
- Telephone
- Client portals
- Alternative communication systems

Communications may include:

- Operational status updates
- Service disruptions
- Contact instructions
- Recovery updates

The Firm utilizes cloud-based systems and third-party vendors for portions of its operations.

These systems may include:

- CRM systems
- Custodial platforms
- Email systems
- File storage systems
- Financial software
- Compliance systems
- Communication platforms

The Firm maintains reasonable due diligence procedures regarding vendor reliability and security.

The Firm maintains electronic records and backup procedures designed to preserve critical data.

Backup procedures may include:

- Cloud redundancy
- Encrypted storage
- Vendor-hosted backups
- Redundant systems
- Secure archival retention

The Firm maintains books and records pursuant to applicable regulatory requirements.

Third Party Vendors

The Firm relies on certain third-party vendors and service providers.

Examples may include:

- Custodians

- CRM providers
- Cloud providers
- Internet providers
- Email providers
- Compliance vendors
- Data providers

The Firm recognizes that third-party disruptions may affect operations and will make reasonable efforts to maintain operational alternatives where practicable.

Third Party Contact Information
(I.E. vendors, banks, order routers, data providers, utilities)
Mercantile Bank: 217-224-8686
Ameren: 800-755-5000
AT&T: 800-727-2100
Employee Contact Telephone Numbers:
Todd Butterfield 217-577-5188 Karrie Butterfield 217-257-5438
Emergency Contact Information
Local Police Department: 217-277-2200
Local Fire Department: 217-656-3231

Annual Testing

The Company will test its disaster recovery/business continuity plan on an annual basis. The Company will maintain written evidence that the plan was tested**.**

The Firm may conduct:

- Operational reviews
- Cybersecurity testing
- Backup verification
- Vendor continuity reviews
- Incident response simulations

Testing may be documented internally

Responsibilities

The Chief Compliance Officer ("CCO") and designated personnel are responsible for:

- Oversight of continuity procedures
- Coordination of response efforts
- Vendor coordination
- Cybersecurity escalation
- Regulatory communication where necessary
- Plan maintenance and review
-

All personnel are responsible for:

- Following emergency procedures
- Protecting Firm systems
- Reporting incidents promptly
- Maintaining secure practices

Limitations

While the Firm maintains continuity procedures reasonably designed to support operations, no continuity plan can eliminate all operational risks or guarantee uninterrupted service.

Certain disruptions may be outside the Firm's reasonable control.

Conclusion

BlackBay Capital Advisors is committed to maintaining operational resilience, protecting client information, and supporting continuity of service through reasonable planning, cybersecurity safeguards, and operational oversight.

This Business Continuity and Disaster Recovery Plan is intended to support the Firm's fiduciary and regulatory obligations while promoting operational stability during periods of disruption.