Business Continuity & Information Technology Security Manual

November 2025

TABLE OF CONTENTS

Business Continuity Plan

Business Continuity Plan

Purpose and Adviser Policy

Capita Financial Network, LLC ("Adviser") has adopted this Business Continuity Plan ("BCP") pursuant to the Investment Advisers Act and the rules and guidance of the U.S. Securities and Exchange Commission ("SEC") and the laws of the States where Adviser is currently registered.

The purpose of this BCP is to define the strategies and plans that will be used by the Adviser during a significant business disruption ("SBD"). An SBD includes any event or situation that significantly impacts the Adviser's ability to provide advisory services to its clients. The BCP outlines Adviser's procedures designed to ensure that critical business functions can continue during and after an SBD and that Adviser can resume operations as quickly as possible. The BCP is prepared to address both internal SBDs, such as a fire in the Adviser's building or the death of key personnel, and external SBDs, such as a natural disaster, terrorist attack, or citywide power disruption. It is also designed to address SBDs of different severities.

In the event of an SBD, it is Adviser's policy to do the following to the extent reasonable and practical under the circumstances:

- Safeguard employee lives and firm property;
- Make a financial and operational assessment;
- Promptly recover and resume operations;
- Protect the firm's books and records; and
- Communicate with its customers and allow them to transact business.

Although the firm does not maintain custody of customer assets, in the event of an SBD, Adviser will assist customers to access their assets at the appropriate broker. In the case of an external SBD, the Adviser's ability to react will depend heavily on access to other organizations and systems, such as the availability of electricity, telephones, Internet and transportation.

In creating this BCP, Adviser has assumed that the firm's designated alternate office(s) will be available, that Adviser has sufficient personnel, and that government agencies and market systems are operational during and after the SBD. If any of these assumptions are incorrect, the Adviser's business could be disrupted until matters are resolved. No contingency plan can

eliminate all risk of service interruption, but the Adviser will continue to assess and update their plans to mitigate all reasonable risks.

Plan Approval, Review, Location and Disbursement

Approval and Review of Plan

The chart located in Appendix A reflects the dates of creation and review and necessary revisions to the BCP. The BCP will be reviewed annually to determine whether any modifications are necessary in light of changes to Adviser's operations, structure, business or location or new regulatory requirements.

The Adviser will test the Business Continuity Plan to identify any weaknesses and gaps at least annually. This may include testing of areas such as: accessing back-up records; hardware functions backup hardware; verification of current contact information and any designated duties for employees, clients and business partners; verification of vendors, service providers, software and equipment; and conforming the firm's business practices to the BCP and regulatory requirements.

Scott Watko, Chief Compliance Officer, is responsible for approving the plan and for conducting annual reviews. After the execution of the annual BCP test, Scott Watko will review and revise Adviser's BCP as necessary to ensure it meets the firm's needs and regulatory requirements. An updated copy of the BCP will be distributed to all of Adviser's employees within forty-eight (48) hours of any amendment.

Plan Location and Access

The Adviser will maintain copies of its BCP, the annual reviews, and any revisions made to the plan. An electronic copy of Adviser's BCP is located on Adviser's Box.com cloud storage in the folder named Compliance>Compliance Officer Files>Business Continuity Plan.

Disbursement of Plan

All employees of Adviser will review the BCP upon beginning their employment. When the BCP is updated, all employees will review the revised plan. The Adviser will periodically train all its employees on the BCP's requirements.

Key Personnel and Succession Plan

Adviser's key personnel and persons responsible for executing this BCP in the event of an SBD are:

- Michael Littledike: mike@capitamail.com
- Zaccary Call: zacc@capitamail.com
- Cassandra Myers: cassie@capitamail.com

In the event that these key personnel die or become incapacitated or otherwise unavailable, the following persons are authorized to execute this BCP and carry on Adviser's business and/or wind down the business: Scott Watko, Chief Compliance Officer, Kelsey Dent, Partner and Director of Financial Services, Tyler Williamson, Partner and Adviser, Bart Wagstaff, Partner and Adviser, Todd Storrs, Wealth Management Director. These persons have been trained on how to execute the provisions of the BCP and carry on the Adviser's business and/or wind down the business.

Business Description

The Adviser is an SEC-registered adviser that transacts business in public equity, fixed income, and fixed annuity products. Adviser provides analysis and advice on securities by making direct or indirect recommendations to clients or by providing research or opinions on securities or securities markets. The Adviser is compensated for providing this analysis and advice. The Adviser is also authorized to execute trades in customer accounts on their behalf.

The Adviser sends all public securities transactions to executing independent brokers, which process and settle their orders. The Adviser does not act as a broker and does not hold client funds or securities.

Office Location

The Adviser's primary office is located at **14658 S. Bangerter Pkwy Ste. 300 Draper, UT 84020**. The main telephone number is **(801) 566-5058**. Employees travel to that office by means of automobile and public transit. The Adviser engages in client meetings, financial planning, asset management services, operations, and income planning at the primary office.

Alternative Physical Location(s) of Employees

In the event of an SBD, the Adviser will move its staff from the affected office(s) to any available space that can be rented to accommodate client meetings. Alternatively, with our use of technology and cloud storage we can effectively conduct business from any location with power and data connections (i.e. phone, internet, etc.) Telephone numbers will remain the same, as we can re-route calls to personal and business cell phones if needed. If the Adviser cannot return to its primary office within a reasonable amount of time following the SBD, it will evaluate whether to permanently move to a new primary office location.

In the event of an SBD involving widespread lack of telecommunications, transportation, electricity, office space, fuel and water, the Adviser will consider its employees' ability to work remotely during the SBD, as well as how employees may work in the absence of telephone and/or Internet access if necessary. The plan calls for employees to work from home in the event of an SBD. Additionally, workspaces at the Littledike and Call residences can be used, as they have backup generators that would help accomplish the work of keeping business operations running.

Customer Access to Funds and Securities

The Adviser does not hold customer funds or securities. Customer funds and securities are held with Charles Schwab and Fidelity Investments, and customers have access to those funds and securities independent of Adviser. The business continuity plans of Charles Schwab, Fidelity Investments, and Orion are available online at:

https://www.schwab.com/legal/continuity

https://www.fidelity.com/customer-service/business-continuity

https://orion.com/business-continuity-plan

In the event of an SBD, the Adviser will continue to handle customer assets as it did before the SBD to the extent possible based on the availability of the applicable custodian's platform.[1]

Data Back-Up and Recovery (Hard Copy and Electronic)

The Adviser maintains its primary books and records and its electronic records at cloud storage provider Box.com. Scott Watko, Chief Compliance Officer, is responsible for the maintenance of these primary books and records.

The Adviser maintains its back-up of books and records at Box.com. Adviser uses an enterprise edition with unlimited storage and has access to proprietary data being simultaneously stored on different Box.com servers around the country to create redundancy and security. These records are primarily digital with governance features of protection from deletion. Scott Watko, Chief Compliance Officer, is responsible for the maintenance of these

[1] *Note: In the event of an SBD, reliance on a single telecommunications service provider could prevent Adviser from performing its obligations. Adviser should consider contracting with multiple carriers in order to have a backup carrier to maintain telephone, email, and fax services.*

back-up books and records. Adviser backs up its records by copying and uploading them and taking them to the cloud storage provider. Adviser backs up its digital records every week.

For the loss of electronic records, Adviser will either physically recover the storage media or electronically recover data from the back-up site.

Operational and Financial Assessments in the Event of an SBD

Operational Risk

In the event of an SBD, the Adviser will immediately assess and identify what means will permit it to communicate with customers, employees, regulators, any custodian institution(s) holding customer funds and securities, and critical business constituents and counterparties. Although the impact of an SBD will determine the means of alternative communication, the Adviser may employ telephone voice mail, secure email, or text messaging. In addition, Adviser will retrieve key activity records as described in Section VIII, above, Data Back-Up and Recovery (Hard Copy and Electronic).

Financial and Credit Risk

In the event of an SBD, the Adviser will determine its financial ability to continue to operate and service its customers. The Adviser will contact the custodian firm, clients and critical banks to apprise them of its financial status. If the Adviser determines that it is unable to fund its operations, it will request additional financing from its bank or other credit sources to fulfill its obligations to customers.

Critical Systems

Adviser's critical systems are those that: (i) allow Adviser prompt and accurate access to client accounts and records, (ii) allow Adviser to communicate investment advice and analysis to customers, and (iii) allow Adviser to receive and transmit orders from or on behalf of customers to Charles Schwab and/or Fidelity Investments for execution.

Adviser has primary responsibility for establishing and maintaining business relationships with customers and transmitting orders from or on behalf of customers to Charles Schwab and/or Fidelity Investments for execution. Charles Schwab and/or Fidelity Investments have responsibility to receive, execute, clear and settle orders from Adviser or its customers.

Adviser has received and reviewed a copy of the business continuity plan of Charles Schwab and/or Fidelity Investments. The custodian has indicated that it will notify Adviser of any material changes in its business continuity plan that might affect Adviser's ability to maintain its business.

Critical Business Constituents, Banks and Counterparties

Adviser has contacted its critical business constituents (businesses with which it has an ongoing commercial relationship in support of its operating activities, such as vendors and banks), and determined the extent to which Adviser can continue its business relationship with them in light of an SBD. Adviser will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services as required. Adviser's critical business constituents include Orion/Townsquare Capital (Sub-Adviser) and centers of influence partners (attorneys, accountants, consultants, etc.).

Adviser requires all its service providers to provide it with copies of their Business Continuity Plans.

Adviser has contacted its bank to determine if they can continue to provide the support that Adviser needs in light of an internal or external SBD. The bank maintaining Adviser's operating account is Chase Bank, www.chase.com.

Adviser has also contacted its critical counterparties to determine if Adviser will be able to carry out its transactions with them in light of an internal or external SBD. Where transactions cannot be completed, Adviser will work with its clearing firm or contact those counterparties directly to make alternative arrangements to complete transactions as quickly as possible.

Communication of SBD to Other Parties

In the event of an SBD, including the death or unavailability of key personnel, the persons executing this BCP will determine the persons that need to be notified about the SBD, including employees, customers, regulators, custodians, and critical business constituents. The persons who need to be notified, and the way in which they will be notified, will vary with the circumstances of the SBD.

During an SBD, Adviser will ensure, to the extent possible, that its website reflects the firm's operational status and contact information. Adviser may place status messages on its website indicating to customers, for instance, the nature of the SBD or the status of its services to customers.

Alternative Communications Plans

Customers

Adviser now communicates with customers using telephone, email, fax, U.S. mail, and in-person appointments. In the event of an SBD, Adviser will assess which means of communication are still available and use the means closest in speed and form (written

or oral) to the means that Adviser used in the past to communicate with the other party. For example, if Adviser has primarily communicated with a party by email, but the Internet is unavailable, Adviser will call the customer on the telephone and follow up where a record is needed with a paper copy in the U.S. mail.

In the case of an expected SBD, such as a forecasted storm, Adviser will consider proactively contacting customers (for instance, by email blast) to determine whether they need to execute any transactions (e.g., fund transfer, wire instructions, closing out positions) in case of an extended outage.

Employees

Adviser now communicates with its employees using phone, text message, social media, and email. In the event of an SBD, Adviser will assess which means of communication are still available and use the means closest in speed and form (written or oral) to the means that Adviser has used in the past to communicate with the other party.

Regulators

Adviser is currently registered as an investment adviser firm with the SEC. Adviser communicates with its regulators using telephone, email, website, and U.S. mail. In the event of an SBD, Adviser will assess which means of communication are still available, and use the means closest in speed and form (written or oral) to the means that Adviser has used in the past to communicate with the other party, including to make any necessary filings, disclosures, etc.

If Adviser cannot contact its regulators, it will continue to file required reports to the extent possible using the means of communication available to it.

In the event of a formal or informal inquiry made by any federal or state regulatory agency during an SBD, Scott Watko, Chief Compliance Officer, will be responsible for receiving all calls and/or all other requests for further review.

Custodians

Charles Schwab and/or Fidelity Investments currently hold the funds and/or securities of Adviser's customers. Adviser currently communicates with these institutions using telephone, email, and US-mail. In the event of an SBD, Adviser will assess which means of communication are still available and use the means closest in speed and form (written or oral) to the means that Adviser has used in the past to communicate with the custodian.

Critical Business Constituents, Banks and Counterparties

Adviser now communicates with its critical business constituents using telephone, email, and websites. In the event of an SBD, Adviser will assess which means of communication are still available and use the means closest in speed and form (written or oral) to the means that Adviser has used in the past to communicate with the other party.

Disclosure of Business Continuity Plan

Customers will receive a copy of a BCP summary disclosure statement upon request (and annually thereafter, if applicable). A copy of the BCP summary disclosure is attached to the BCP. Adviser will mail it to customers upon request.

DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN DISCLOSURE STATEMENT

Capita Financial Network, LLC ("Adviser") has adopted a Business Continuity Plan ("BCP") pursuant to the Investment Advisers Act and the rules and guidance of the U.S. Securities and Exchange Commission ("SEC") and the laws of the states where the Adviser is registered. The purpose of the BCP is to define the strategies and plans that will be used by Adviser during a significant business disruption ("SBD"). The BCP is prepared to address both internal SBDs, such as a fire in Adviser's building, and external SBDs, such as a natural disaster, terrorist attack, or citywide power disruption.

Our Business Continuity Plan

In the event of an SBD, Adviser will safeguard employee lives and firm property. Adviser will work to re-establish the systems necessary to quickly recover and resume operations, protect Adviser's books and records and allow Adviser's customers to transact business to the extent reasonable and practical under the circumstances. Adviser's BCP addresses: alternate office locations, customer access to funds and securities, financial and operational assessments, data backup and recovery, critical systems, alternative communications with customers, employees, regulators, and critical business constituents.

Contacting Adviser and Accessing Funds and Securities

If you are not able to contact Adviser through our regular telephone number (801) 566-5058, please contact us by email at info@capitamail.com. For questions relating directly to accessing your funds and securities, please contact Charles Schwab at 877-519-1403 or schwab.com, and/or Fidelity Investments at 800-343-3548 or Fidelity.com.

Varying Disruptions

SBDs can vary in their scope, from only our firm to a single building housing our firm, the business district where our firm is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only our firm or a building housing our firm, we intend to transfer our operations to a local site when needed and expect to recover and resume business within a 48-hour time period. In a disruption affecting our business district, city, or region, we intend to transfer our operations to a site outside the affected area and recover and resume business within a five-day time period. In either situation, we plan to continue in business. However, the ability of Adviser to fully function is dependent on outside sources outside of its control, including the availability of electricity, telephones, Internet, transportation, and the functioning of institutions and markets worldwide. Nothing in Adviser's BCP or this disclosure statement is intended to provide a guarantee or warranty regarding the actions or performance of Adviser.

Additional Information

If you have questions about our business continuity planning, please contact us at 801- 566-5058.

Appendix A

Effective Date	Description of Action	Name & Title of Firm Employee/Executive
May 22nd, 2018	Creation of BCP	Lucas Allen, Chief Compliance Officer
Mar/Apr 2022	Review and revise	Lucas Allen, CCO with Scott Watko
July 22, 2022	Execution of BCP Test	Scott Watko, Chief Compliance Officer
July 21, 2023	Execution of BCP Test	Scott Watko, Chief Compliance Officer
August 21, 2024	Execution of BCP Test	Scott Watko, Chief Compliance Officer
January 15, 2025	Review and revise	Scott Watko, Chief Compliance Officer
August 21, 2025	Execution of BCP Test	Scott Watko, Chief Compliance Officer

APPENDIX B

Service Provider Name	Description	Contact Name	Contact Email	Contact Phone
Betsy Voter (Michael Best Attorneys at Law)	Outside Legal council	Betsy Voter	btvoter@ michaelbest.com	801-924-4105
TownSquare Capital	Third-party Asset Manager	Michael Folker	michael@ townsquarecapital.com	385-375-8619
Salesforce-Pardot	CRM and Mass email system	Joe Riley	joseph.riley@ salesforce.com	
Orion	Portfolio Accounting		sme-salesforcesupport@ orion.com	
Nitrogen	Risk Tolerance & Investment Proposals	Luke Cook	lcook@ riskalyze.com	530-748-1660
Zoom	Video conferencing and Webinar software	Brian Sidney	brian.sidney@ zoom.us	
eMoney	Financial Planning software	Jeff DiGiovanni	jdigiovanni@ emoneyadviser.com	610-684-4607
Message-watcher	Email archiving and supervision	Craig Dinan or Kurt Larson	support@ messagewatcher.com	720-394-0161 (Craig)
G-Suite	Email client, team collaboration tool	Wally Overstreet	wallyo@ google.com	
Holistiplan	Tax Analysis software for clients		help@ holistiplan.com	
Box.com	Cloud Document Storage	Hailey Adams	hadams@ box.com	530-913-9289

Allegis	Contact for Annuity clients	Dean Hamilton	dean.hamilton@ allegisag.com	801-826-3911
Charles Schwab	Account Custodian	Dedicated Team	ASIG17@ schwab.com	866-738-9111
Fidelity Investments	Account Custodian	Dedicated Team	WestGreen@ fmr.com	401-292-6338
Ring Central	Phone/internet service	Hazel Solete	hazel.solete@ ringcentral.com	800-574-5290
UI Charitable Advisors	DAF Custodian	Hyrum Grenny	support@ uicharitable.org	385-286-5900
Bamboo?	HR and Payroll	Stephanie Lo Piccolo	privacy@ banboohr.com slopiccolo@ bamboohr.com	801-724-6600 ext. 6791
Lift Property Management	Property Management for Primary Office	Scott Alder	scott@ managedbylift.com	(801) 664-0620

Disaster Recovery Plan

Disaster Recovery Plan

Introduction

Capita Financial Network has adopted this Disaster Recovery Policy. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope of Policy

The scope of this disaster recovery plan addresses technical recovery only in the event of significant disruption. All personnel of Capita Financial Network must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce. The disaster recovery plan should be tested annually to maintain its integrity.

Considerations

- A disaster may occur at any time, not necessarily during work hours
- Capita Financial Network should establish and implement processes and procedures for responding effectively to emergencies or other occurrences that damage systems containing PII / sensitive data
- Systems that contain PII / sensitive data can be affected or destroyed in many ways, such as:
    - Flooding
    - Fire
    - Loss of power
    - Acts of God: Tornado, tsunami or hurricane
    - Unauthorized access or malicious activity
    - Vandalism

Policy Statement

It is the policy of Capita Financial Network to establish and implement processes and procedures to create and maintain retrievable exact copies of PII / sensitive data.

Disaster Recovery Procedures

Phase 1 - Response

- Identify team members/roles that will be needed for recovery

- Contact required personnel
- Determine recovery strategies/options to be taken based on disaster type

Phase 2 – Recovery

- Implement recovery procedures/failover
    - Identify restoration procedures
    - Assess risk for each procedure
    - Implement procedures

Phase 3 – Validation

- Validate integrity of restored data and the accessibility of that data
    - Test the recovery and communicate to organization

Pre-disaster measures

- Backup all PII / sensitive data with accordance to Capita Financial Network's backup policy
- Test integrity of backups (Daily software verifications, with no less than monthly test restores and audits on new servers and quarterly for all servers)
- Protect by uninterruptible power supplies ("UPS") all servers and other critical equipment from damage in the event of an electrical outage
- Provide annual training in disaster preparation and recovery and knowledge of responsibilities in the event of a disaster (share the Incident Response Plan with employees found in the Information Security Policy)

Disaster Recovery Teams and Responsibilities

In the event of a disaster, different groups will be required to assist in the effort to restore normal functionality to the employees of Capita Financial Network.

The different groups and their responsibilities could include:

Disaster Recovery Lead(s)

- Technical Account Manager, Professional Services Manager, & Security/Backup & Disaster Recovery Manager manages all processes of the disaster recovery plan

Disaster Recovery Team

- Technical Account Manager: Communicates with CFN Management and workforce and IT Teams strategic goals and resolutions.
- Professional Services Manager: Reviews environment and identifies strategy to minimize damage and rebuild long term or temporary technical environment to get back to production as soon as possible.
- Security/BDR Manager assesses the situation to build a strategy to get the client back up and running again with the Professional Services Manager goals on infrastructure rebuild. Also assesses security strategy appropriate to threat. Coordinates and executes the threat removal/recovery.

IT Department

- Handle all IT related processes of the DR plan
- In the event of a disaster that does not require migration to standby facilities, the team will determine which servers are not functioning at the primary facility
- If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact
- Install and implement any tools, hardware, and systems required for recovery

Operations

- Ensure that the Disaster Recovery Team Lead is held accountable for his/her role
- Assist the Disaster Recovery Team Lead in his/her role as required

Finance Department

- Ensure there is sufficient cash on-hand or accessible to deal with small-scale expenses caused by the disaster
- Ensure there is sufficient credit available or accessible to deal with large-scale expenses caused by the disaster. These can include paying for new equipment, repairs for primary facilities, etc.
- Review and approve Disaster Teams' finances and spending

Disaster Recovery Leads

Technical Account Manager:	Tyson Bottorff
Professional Services Manager:	Tyler Voorheis
Security/Backup & Disaster Recovery Manager:	Seth Madsen

The Disaster Recovery Lead is responsible for making all decisions related to the disaster recovery efforts. This person's primary role is to guide the disaster recovery process. All other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs.

Disaster Recovery Lead Role and Responsibilities:

- Make the determination that a disaster has occurred and trigger the DRP and related processes.
- Be the single point of contact for and oversee all of the disaster recovery processes.
- Determine what systems and processes have been affected by the disaster.
- Communicate the disaster to the other disaster recovery teams.
- Organize and chair regular meetings of the Disaster Recovery Team leads throughout the disaster.
- Create a detailed report of all the steps undertaken in the disaster recovery process
- Present to the Management Team on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage all DRP tests and author all DRP updates.
- Notify the relevant parties once the disaster is over and normal business functionality has been restored.

Disaster Recovery Team

Name	Role/Title	Company	Work Phone Number	Mobile/Home Phone Number
Tyson Bottorff tysonb@equinoxits.com 562 West 800 North, Ste 201 Orem, Utah 84057	Technical Account Manager	Equinox	801-426-7800	801-822-8233
Tyler Voorheis tylerv@equinoxits.com 562 West 800 North, Ste 201 Orem, Utah 84057	Professional Services Manager	Equinox	801-426-7800	801-473-7146
Seth Madsen sethm@equinoxits.com 562 West 800 North, Ste 201 Orem, Utah 84057	Security/BDR Manager	Equinox	801-426-7800	310-740-6446
Anna Joel annaj@equinoxits.com 562 West 800 North, Ste 201 Orem, Utah 84057	Operations Manager	Equinox	801-426-7800	801-358-7179

System and Application Criticality

Capita Financial Network provides several critical systems to service its business needs. It is important to note that this DRP attempts to classify and categorize the many systems and applications supported by CFN for the purpose of offering a tiered approach to the restoration of the services and systems in the event of a disaster. If a disaster does occur, the systems and applications will be restored in tier order as follows:

- Tier A –The system is critically fundamental to the operation of the business and must be restored immediately (within 4-24 hours, as reasonable).
- Tier B – The system is important to the daily business operations but may be out of service for 1 business day and up to 3 business days in case of a serious catastrophe as reasonable.
- Tier C – The system is not required for daily business operations and can run successfully for an extended period (3 business days or more) without the system being available.

Disaster Recovery System Criticality

System / Application	Function	Consequences of Disruption	Workarounds / Alternatives	Primary Contact	Priority Tier
List name of system or application	Describe the function or purpose of the system.	Explain what would happen if the system was unavailable.	List any other method that would allow your business to continue to access the data or use the system during a disruption.	List the primary contact for the listed system.	Assign a priority tier (A, B, or C) based on the definition.
C3CMS	Viewing and Recording Cameras	Users would be unable to view cameras	None/Look at another camera vendor	Ideacom Support	Tier A
AD01	Active Directory	All authentication/ DNS stops	Recover From Backup	Equinox IT Services	Tier A
Adobe Acrobat	PDF Creation/Editing Software.	Unable to create/edit PDFs.	Utilize alternate PDF editing software (CutePDF, PDFforge).	Adobe Support	Tier B
Adobe Photoshop and Creative Cloud	Image Editing Software.	Marketing wouldn't be able to edit videos and other material	Utilize alternate creating software (GIMP, other).	Adobe Support	Tier C
Box	Cloud File Storage	Unable to save or access files.	Send files using another method, store files in OneDrive/SharePoint	Box Support	Tier A
Google Workspace	Emailing, Workspace Apps	Unable to Email/utilize drive, docs, slides, etc…	None / look into M365 or other email platforms	Google Support	Tier A
Microsoft 365 Apps for Business	Office Software on WS	End users can't use Word, Excel, Outlook, etc.	Reinstall with existing keys that are documented. Use web app for email.	Equinox IT Services	Tier A
RingCentral Meetings	Conferencing software.	Unable to attend/make conference calls from board rooms	Move meeting from LifeSize to other service (Zoom, Teams, etc.)	RingCentral Support	Tier B

WatchGuard Firewall	WG M290	Internet goes down. VPN connection would go down.	Currently just replace and restore. HA units are available.	WG Support & Equinox IT Services	Tier A
Zoom	Teleconferencing Software	Unable to attend/make conference calls.	Use Teams or another software in the meantime.	Zoom Support	Tier B
Canva	Design software used by both Marketing and Ops.	Marketing is no longer able to design event flyers, office forms no longer able to be updated.	Use Adobe or another software	Canva Support	Tier C
RingCentral	Softphones on every endpoint, used for calls, fax, and texting	Clients unable to contact CFN, unable to use main line to contact anyone.	Use personal cell phones or email (check with compliance)	Rylie Reynolds	Tier A
SSA Benefit Calculator (website)					Tier C
TellerScan	Check scanning software for Fidelity	Unable to scan checks into Fidelity	Mail-in checks directly (FedEx)	Equinox/Fidelity Support	Tier C
Schwab (website)	Primary custodian	Unable to trade, transact, view client accounts			Tier A
Fidelity (website)	Primary custodian	Unable to trade, transact, view client accounts			Tier A
SalesForce	CRM that houses all customer information	Lose access to customer information and wouldn't be able to add new info	None / Look into another CRM solution	Rylie Reynolds	Tier A

Bamboo HR	HR platform; payroll, employee records, etc.	Payroll would be delayed, hiring would be impacted	Manual check payments to employees	Mallhory Jones	Tier A
Keeper Security	Password management solution used by all employees to store work credentials	Unable to login to websites and other critical software	Use offline version (mobile/desktop app), reset credentials if needed	Equinox IT Services	Tier A

Disaster Recovery Steps

1. Set the DRP into motion after the Disaster Recovery Leads have declared a disaster. Schedule A to this DRP sets forth our Primary Site Failure Plan
2. Identify and follow workarounds so business can resume ASAP
3. Determine the extent of the damage and whether additional equipment/supplies are needed
4. Determine how long it will be before service can be restored, and notify required personnel
5. Replace hardware as necessary to restore service
6. Retrieve and upload backup files, if necessary, to restore service
7. Ensure that backup procedures are followed
8. Verify the integrity of data restored and the ability for workforce members to access
9. Coordinate activities to ensure that the most critical tasks are being supported as needed
10. Keep administration, information personnel, and others informed of the status of the emergency mode operations
11. Coordinate with administration and others for continuing support and ultimate restoration of normal operations
12. Follow up with an after-action review to make plans for always continuing to improve

Plan Testing

The DRP should be updated every 6 months or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead is responsible for updating the entire document and is permitted to request information and updates from other employees and departments within the organization to complete this task.

Capita Financial Network is committed to ensuring that this DRP is functional. The DRP should be tested every year to ensure that it is still effective. Testing may include, but is not limited to, reviewing existing assets and redundancies and making changes as necessary.

Creation Date: 10/06/2025

Effective Date: 11/20/2025

Last Revision Date: 11/20/2025

SCHEDULE A

PRIMARY SITE FAILURE PLAN

DAY ONE

- Internal communication is handled as follows:
    - Scott and Rylie as primary contacts to coordinate the notification of the executive team and Equinox IT.
    - Communicated to other partners and staff as appropriate
- Email is hosted by a third party and email communications should not be disrupted even if primary office is unavailable.
- Scott and Rylie conduct an initial assessment of the viability of the primary office.
- Communicate to all staff to work from their home office. Essential functions have already been established for all employees to work from home. See WFH Policy.
- Should Servers / VPN connection to primary site be inaccessible, users will resort to utilizing other means for file shares such as Microsoft OneDrive/SharePoint.

DAY TWO

- Scott and Rylie to coordinate with Equinox IT to Assess viability and recovery time of primary systems. If timing is greater than ten days, acquire alternative systems and install hardware and software to resume operations. Establish daily email to inform key contacts of timeline to interim and full recovery.
- DFS and Distributed Active Directory is utilized across a secure Wide Area Network (WAN) in real time. If one site fails, the other site can handle all functions.
- All servers are backed up hourly with backups going to Equinox's private cloud. M365 environment is backed up daily with backups going to cloud service.
- If both offices are unavailable, offsite backup will be restored hardware provided by Equinox for user access until permanent space can be reestablished.

SUBSEQUENT

Depending on recovery time of primary office, assess need for new temporary or primary office. Policy has been established whereby all firm personnel can immediately commence business operations in each employee's home office. The server would be accessible in a separate temporary location at Equinox IT Services located at 562 West 800 North, Suite 201, Orem, Utah 84057.

At new site, if necessary, restore systems.

Written Information Security Policy

Written Information Security (WISP) Policy

Statement of Policy

The objective of Capita Financial Network ("Capita", "The Company") in the development and implementation of this comprehensive Written Information Security Policy ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personally identifiable information ("PII") of customers, clients and employees as well as sensitive company information that could be harmful if unauthorized access were to occur. The WISP sets forth a procedure for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII and sensitive company information.

*The use of the term **employees** will include all of The Company's owners, partners, managers, employees, all independent contractors, temporary employees and interns.*

Purpose of Policy

The purpose of the WISP is to better:

1) Ensure the security and confidentiality of PII of customers, clients, employees or vendors as well as **sensitive company data** which includes emails, confidential company information (i.e. company proprietary information and highly sensitive information, etc.), employee information, payroll and the like;

2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and

3) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud or harm to The Company.

Scope of Policy

In formulating and implementing the WISP, Capita Financial Network has addressed and incorporated the following protocols:

1) Identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII and sensitive company data.
2) Assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the PII and sensitive company data.
3) Evaluated the sufficiency of existing policies, procedures, customer information

systems, and other safeguards in place to control risk.

4) Designed and implemented a WISP that puts safeguards in place to minimize identified risks.
5) Implemented regular monitoring of the effectiveness of those safeguards.

Security Safeguards

The following safeguards are effective immediately. The goal of implementing these safeguards is to protect against risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing PII or sensitive company data.

Administrative Safeguards

Security Officer

The Company has designated **Scott Watko, Chief Compliance Officer ("CCO")**, as the Security Officer responsible for implementing, supervising, and maintaining the WISP.

The Security Officer's key duties include:

- Implementing the WISP and all associated **Security Safeguards**.
- Providing training on data security to all employees with access to PII and sensitive company data, including annual refresher training and onboarding training for new hires.
- Monitoring compliance with the WISP safeguards and employee adherence.
- Assessing Third-Party Service Providers' security practices, ensuring contracts require appropriate protection for PII and sensitive data.
- Reviewing and updating security measures at least annually or when significant changes to business practices occur.
- Investigating, reviewing, and responding to all actual or suspected security incidents.

Security Management

All security measures shall be reviewed at least annually, or whenever a material change in business practices may expose PII or sensitive company data to new risks. This includes conducting a formal security risk assessment, documenting findings, and implementing recommended improvements.

Risk Assessment Process:

Under the direction of the Security Officer (or delegate), Capita will perform an annual WISP security risk assessment that:

- Identifies known and reasonably foreseeable internal and external threats.
- Evaluates the likelihood and potential impact of these threats
- Assesses the adequacy of current administrative, technical, and physical safeguards
- Assigns risk severity ratings and sets timelines for remediation of significant risks
- Is documented, reviewed by senior compliance personnel, and retained for at least five years

The Security Officer is responsible for conducting the review, communicating results and recommendations to the executive team, and documenting any material changes to the WISP or related procedures.

Minimal Data Collection

The Company collects PII from clients, customers, and employees only as necessary to conduct legitimate business transactions and comply with all applicable federal, state, and local regulations.

Capita collects PII solely to:

- Fulfill fiduciary and regulatory obligations.
- Deliver investment advisory or insurance services.
- Meet contractual or legal requirements.

Data collection practices are reviewed at least annually to ensure ongoing compliance with regulatory requirements.

Information Access

Access to records containing PII and sensitive company data is restricted to personnel whose job functions require such access for legitimate business purposes. Pre-employment screening is conducted to help safeguard this information.

Access controls apply to electronic systems, physical files, and environments storing PII or sensitive data and must:

- Be limited to personnel with a legitimate, role-based business need.

- Be audited as needed to verify appropriate access levels.
- Be revoked immediately upon employee termination or job function changes.
- Be logged and regularly reviewed to detect unauthorized access.

The CCO or delegate maintains records of all access approvals and revocations, and oversees changes to access privileges. Access attempts may be monitored periodically to ensure compliance.

Employee Termination

Upon termination of employment or contract (voluntary or involuntary), Capita requires immediate revocation of all access to PII and sensitive company data and return or secure deletion of all related materials in the former employee's possession.

Requirements for Terminated Employees:

- Return all records containing PII or sensitive data in any form, including information on laptops, portable devices, media, files, records, and work papers.
- Surrender all keys, IDs, access codes, business cards, and any other items granting access to company premises or systems.
- Remote electronic access—including voicemail, email, internet, and passwords—must be disabled immediately.

Offboarding Procedures (completed on the same business day or as soon as feasible):

- Revoke all physical and digital access credentials (network accounts, email, file shares, third-party platforms).
- Retrieve all company-issued equipment and physical documents containing sensitive or proprietary data.
- Instruct terminated employees to return or confirm destruction of any business data stored on personal devices.
- Disable remote access, email forwarding, and voicemail systems.
- Conduct an offboarding checklist review involving the Compliance, HR, and Operations departments.
- Maintain written records of access revocation and asset recovery in the employee's compliance file.

Security Training

All personnel—including owners, partners, managers, full-time employees, interns, independent contractors, and temporary workers—with access to PII or sensitive company data must complete mandatory information security training.

Training Requirements:

- **Timing:** New hires must complete training within 10 days of onboarding, and all employees must complete training at least annually.
- **Content:** Training covers key security topics such as phishing awareness, best password practices, remote work safeguards, incident reporting, and proper data handling.
- **Evaluation:** Employees must pass an assessment or knowledge check to demonstrate understanding.
- **Documentation:** The CCO (or delegate) will maintain training records, including dates and assessment results.
- **Updates:** Additional training may be required to address emerging threats, incidents, or regulatory changes.

WISP Distribution

A copy of the WISP shall be provided to all current employees and new hires on their first day of employment. Employees are responsible for electronically attesting that they have received and agree to comply with the WISP.

The CCO is responsible for:

- Distributing the WISP to all supervised persons and employees upon hire and whenever material updates occur.
- Ensuring each recipient electronically attests to receipt and understanding of the WISP.
- Storing the current WISP in a centralized, accessible location (e.g., compliance intranet or secure drive).
- Providing access to the most current WISP version upon request.
- Maintaining a log of all acknowledgments and re-circulating the policy following significant regulatory, operational, or procedural changes.

Contingency Planning

All systems storing PII and/or sensitive company data must be backed up at least nightly. Backups must be encrypted and stored offsite to ensure data security and availability.

Capita maintains a documented Business Continuity Plan ("BCP") that outlines roles, responsibilities, and procedures to restore access to PII, sensitive data, and critical operational systems in the event of a disruption, including cybersecurity incidents, natural disasters, or infrastructure failures.

Key elements include:

- Nightly encrypted backups of core business systems and client records.
- Secure offsite or cloud-based storage of backups to enable rapid restoration.
- Defined Recovery Time Objectives ("RTOs") and Recovery Point Objectives ("RPOs") for mission-critical systems, subject to the capabilities and limitations of third-party vendors' platforms.
- Annual testing of disaster recovery capabilities and documentation of outcomes.
- A clear incident response communication plan for notifying internal teams, custodians, or regulators if material service disruptions or data losses occur.
- Assignment of responsibility to the CCO for coordinating periodic reviews and improvements to the plan.

Security Incident Procedures & Emergency Operations

Capita maintains documented procedures to respond promptly and effectively to security incidents and emergencies involving personal data, confidential business information, or critical systems.

Security Incident Definition:
A security incident is any unauthorized access, use, disclosure, alteration, destruction of personal or company data, or any event that compromises the availability, confidentiality, or integrity of systems managing such data.

Incident Reporting:
All employees, contractors, and supervised persons must immediately report any actual or suspected security incident to their supervisor, the CCO, or the designated Security Officer.

Reportable Incidents Include, but Are Not Limited To:

- Unauthorized access to client, firm, or system data.
- Phishing, malware, or ransomware attacks.
- Loss or theft of devices containing sensitive or personal information.
- Accidental disclosure or exposure of sensitive information.
- Account compromise or other suspicious activity

Incident Response Workflow

Upon Receiving a Report, the Security Officer Will:

- Log the incident in the firm's Security Incident Register.
- Initiate an investigation to assess the scope, severity, and impact.
- Implement containment, mitigation, and remediation actions.
- Determine legal or regulatory obligations, including whether notification to clients, custodians, or authorities is required.
- Notifications will be made within applicable timeframes (e.g., SEC's 72-hour rule, state data breach laws).
- Conduct a root cause analysis to identify and address underlying issues.
- Update policies or controls as needed to prevent recurrence.

Documentation and Follow-Up:

- All incidents must be documented using the firm's Security Incident Report Form.
- Incident records will be reviewed annually by senior leadership as part of compliance oversight and to inform updates to the firm's WISP.

Emergency procedures also include up-to-date employee and critical vendor contact information, key account details, and operational protocols to ensure business continuity.

Data Sensitivity Classification

To protect the integrity and privacy of information, Capita treats all data as *Confidential* by default. Formal data classification is performed on an as-needed basis—most critically during incidents such as a data breach or security assessment, when the nature and sensitivity of the affected data must be determined.

Capita's Data Classification Levels

These levels provide a framework to categorize data based on sensitivity, regulatory

requirements, and potential impact. While not every piece of data is pre-assigned a classification, these categories guide our response and handling protocols:

- **Confidential:** Data that, if accessed or disclosed without authorization, could cause significant harm to clients, employees, or the firm. This includes PII such as Social Security Numbers and account numbers, firm financials, investment strategies, passwords, client contracts, and regulatory correspondence. When identified, this data must be encrypted both in storage and in transit and access is restricted to authorized personnel only.
- **Internal Use Only:** Non-public information intended for use within Capita, such as HR policies, training materials, internal procedures, and system configurations. This data may be shared internally, but not externally without prior approval.
- **Public:** Information explicitly approved for public disclosure, including website content, marketing materials, and regulatory filings like Form ADV.

All personnel are expected to treat all data with a high degree of care and default to a *Confidential* handling posture unless otherwise directed. The CCO is responsible for reviewing and updating the classification framework periodically. New systems, forms, and data types will be assessed and classified when necessary, particularly during the approval process or in response to a data incident.

Third Party Service Providers

Any service provider or individual ("Third Party Service Provider") with access to files containing PII or sensitive company data must protect that information in accordance with The Company's standards. Examples include vendors providing off-site data backup, website hosting, credit card processing, record storage, IT support, or contractors with authorized access.

Requirements for Third Party Service Providers with Access to PII or Sensitive Data:

- Complete and sign Capita's **Due Diligence Questionnaire** that includes:
  - A documented security risk assessment completed prior to engagement.
  - Confidentiality provisions.
  - Information security controls aligned with industry standards.
  - Breach notification timelines and cooperation clauses.
- Undergo **annual reassessments** to verify ongoing compliance.

- Notify Capita within 72 hours of any actual security incidents involving company or client data.

  The CCO (or designee) will maintain and annually review a list of all vendors with access to protected data as part of the compliance program.

Physical Safeguards

Facility Access Controls

Capita implements physical safeguards to protect PII and sensitive company data at all office locations and any location where such data is accessed, stored, or processed. These safeguards are designed to prevent unauthorized physical access, ensure data security, and support compliance with applicable laws and regulations.

The following physical security protocols apply:

- **Facility Access Control:** Office entry is restricted and managed through Alta Open, a secure keycard app issued only to authorized personnel. After-hours access is limited and logged where applicable.
- **Secured Systems and Equipment:** All systems and devices that access or store PII or sensitive data must be physically secured when unattended. Portable equipment and storage media must be locked or otherwise secured.
- **Locked Storage:** Paper records and physical files containing PII or proprietary company data must be stored in locked cabinets when not in use.
- **Clean Desk Policy:** Employees are required to maintain a clean desk environment. No confidential information may be left unattended or unsecured during or outside of business hours.
- **Visitor Restrictions:** Visitors are not permitted in areas where sensitive data is stored or accessed unless escorted by authorized personnel. Access must be documented and monitored.
- **Secure Disposal:** Documents containing sensitive or confidential information must be shredded or securely destroyed when no longer required.
- **Service Provider Oversight:** Cleaning crews and third-party service providers must be screened and supervised when working in areas containing sensitive data.
- **Remote Locations:** Remote offices and offsite locations are subject to periodic audits by the CCO or their delegate.

- **Access Records:** The Security Officer maintains a record of all physical security access credentials, including lock combinations, passcodes, and keys, along with a list of employees authorized to access secured areas and systems.

These physical security measures are an essential part of Capita's broader information security program and are designed to ensure the confidentiality, integrity, and availability of sensitive data across all locations.

Network Security

Capita implements a range of security safeguards to protect PII, sensitive company data, and critical systems from unauthorized access, data breaches, and malicious activity. These safeguards apply across all office locations, remote environments, and devices connected to the Capita network.

Key security controls include:

- **System Isolation and Firewalls:** Systems that access or store PII and sensitive data are logically segmented and protected by commercial-grade firewalls and router configurations to prevent unauthorized external access.
- **Endpoint Protection:** All company-managed devices are equipped with up-to-date antivirus and anti-malware tools. Operating systems and applications must be regularly patched in accordance with vendor recommendations or IT directives.
- **Encryption and Device Security:** All portable devices must use full-disk encryption and be physically protected when in transit or unattended. Devices must meet Capita's current security standards to connect to the network.
- **Device Compliance Checks:** Any device accessing Capita's network or systems is subject to periodic audits to ensure compliance with security requirements. Non-compliant devices may be denied access until remediated.
- **Remote Access Controls:** Remote access (e.g., home offices, mobile devices) to the company's network must be established through a secure VPN and require multi-factor authentication ("MFA").
- **Role-Based Access:** Network access is granted based on job responsibilities. Administrative privileges are limited to authorized personnel only.
- **Wireless Security:** Business Wi-Fi networks must be password-protected, encrypted using WPA2 or higher, and regularly reviewed for unauthorized access or vulnerabilities.

- **Vulnerability Management:** Capita performs periodic vulnerability scans and device audits to identify and remediate security risks across its network and infrastructure.
- **Environmental Protections:** Servers and critical network equipment must be housed in environmentally controlled, secure locations to protect against physical damage.
- **Log Monitoring:** Network activity and system access logs are captured and reviewed regularly by the CCO or designated IT partners to detect unauthorized access or suspicious behavior.

These controls form the foundation of Capita's cybersecurity program and ensure ongoing protection of firm and client data across all systems and environments.

Technical Safeguards

Access Control

Access to PII, sensitive company data, systems, and applications is restricted based on job function, ensuring users have only the minimum access necessary to perform their responsibilities. Only approved and active users with unique login credentials are authorized access; shared accounts are strictly prohibited.

Capita enforces the following access control and data protection procedures:

- All employees are assigned unique user accounts and passwords tied to their roles.
- Access to sensitive or client-specific data requires explicit approval from the CCO or a designated manager.
- Role-based access permissions are defined, maintained, and limited to the minimum necessary for job responsibilities.
- Access rights are reviewed at least annually and upon job changes, transfers, or termination.
- Upon employee separation, all system access must be revoked on the same business day.
- All system access requests and changes are documented and logged.
- Automatic session timeouts, lock screens, and logoff procedures are implemented across all endpoints and systems to prevent unauthorized access.

- A strong password policy is enforced, requiring complex passwords (minimum 12 characters with alphanumeric and symbol requirements), regular expiration, and prevention of reuse.
- All access attempts are logged and reviewed regularly for suspicious activity as part of routine monitoring.

Computer Use

All Capita employees are provided with an Equipment and IT Use Policy**,** which outlines the acceptable and unacceptable use of Capita's computing resources. Employees are required to acknowledge and sign this policy upon hire and annually thereafter.

Capita personnel must use company computing devices and systems in a manner consistent with their job responsibilities and Capita's Written Information Security Policy.

Violations of this policy may result in disciplinary action, up to and including termination.

Data Disposal

Capita ensures that written and electronic records containing PII or sensitive company data are securely destroyed or deleted at the earliest opportunity, consistent with business needs and legal or regulatory retention requirements.

Data disposal procedures include:

- **Physical Records:** Paper documents containing PII or confidential business information must be shredded using cross-cut shredders or securely destroyed by an approved third-party vendor.
- **Electronic Data:** In the rare instance that files must be permanently deleted, it will be done using secure deletion tools to prevent recovery. Decommissioned devices must be securely wiped, degaussed, or destroyed under the supervision of Capita's IT team or a vetted vendor.
- **Retention Schedule:** Unless otherwise required by law or regulation, records will be retained for a minimum of five years. After this period, they must be securely disposed of.

- **Vendor Oversight:** Third-party vendors used for data destruction must sign Capita's Due Diligence Questionnaire and, when applicable, provide a certificate of destruction.

- **Documentation:** Destruction of high-sensitivity records must be logged and retained by the CCO for at least five years.

The CCO is responsible for overseeing the implementation of secure disposal procedures and ensuring that all supervised persons understand their obligations for protecting data throughout its lifecycle.

System Activity Review

Capita maintains both technical and procedural controls to ensure that all systems storing or accessing PII and sensitive company data are continuously monitored for unauthorized or abnormal activity.

Key requirements include:

- **System Logging:** All systems containing client or firm-sensitive data must log and store user activity. This includes CRM platforms, email systems, custodian portals, compliance systems (e.g., MessageWatcher), and firm-managed file servers.

- **Periodic Review:** System activity logs are reviewed at least monthly by the CCO or a designated IT/compliance delegate as part of Capita's ongoing compliance and cybersecurity programs.

- **Review Focus:** Log reviews are designed to detect:
    - Unauthorized access attempts.
    - Logins from unrecognized devices or IP addresses.
    - After-hours or anomalous activity.
    - Repeated failed login attempts.

- **Incident Response:** Any findings of unauthorized access are documented in a System Activity Review Log. Material anomalies are escalated to the appropriate incident response procedures and reported to the Data Security Coordinator.

- **Retention Requirements:** All system logs must be retained for a minimum of three years or longer if required by regulation.

- **Automation:** Automated alerts may be enabled for critical systems where available (e.g., CRM, Orion, Schwab, Microsoft 365) to support real-time threat detection.

Encryption

To protect PII and sensitive company data, Capita requires encryption for data when stored on portable devices or transmitted over public or wireless networks.

Capita's encryption standards and practices include:

- **Backups:** All data backups—whether stored onsite or transferred to offsite or cloud environments—must be encrypted throughout their lifecycle.
- **Cloud Services:** Only Capita-approved cloud platforms may be used for storing or accessing sensitive data. These platforms must support encryption for both data at rest and in transit. Use of unapproved cloud storage or collaboration tools is not allowed.
- **Key Management:** Encryption keys must be securely stored and managed with access restricted to authorized personnel. Shared encryption keys are prohibited unless explicitly documented and protected.
- **Monitoring and Enforcement:** The CCO or designated IT provider is responsible for verifying compliance with encryption requirements through periodic checks and enforcing remediation where necessary.

Capita is committed to maintaining encryption protocols that meet or exceed industry standards to ensure the confidentiality and integrity of sensitive data.

Management of Policy

The management and oversight of this policy, including key dates and approvals, are documented as follows:

Last Review Date: 08/18/2025

Approved by: Scott Watko

Cyber and Data Security Incident Response Plan

Cyber and Data Security Incident Response Plan

Goals for Cyber Incident Response

When a cyber security incident occurs, timely and thorough action to manage the impact of the incident is critical to an effective response process. The response should limit the potential for damage by ensuring that actions are well known and coordinated. Specifically, the response goals are:

1. Preserve and protect the confidentiality of constituent and employee information and ensure the integrity and availability of Capita Financial Network systems, networks and related data.
2. Help Capita personnel recover their business processes after a computer or network security incident or other type of data breach.
3. Provide a consistent response strategy to system and network threats that put the firm's data and systems at risk.
4. Develop and activate a communications plan including initial reporting of the incident as well as ongoing communications, as necessary.
5. Address cyber related legal issues.
6. Coordinate efforts with external Computer Incident Response Teams and law enforcement.
7. Minimize reputational risk to the firm.

Purpose and Scope

This publication provides practical guidelines on responding to cyber security and data breach incidents in a consistent and effective manner. The plan establishes a team of first responders to an incident with defined roles, responsibilities, and means of communication.

While this plan is primarily oriented around cyber-related incidents and breaches, it can also be utilized for data breaches that are not related to computer systems.

Incident Response Team (IRT)

A team comprised of company staff, advisors, and service providers shall be responsible for coordinating incident responses and known as the Incident Response Team (IRT). The IRT shall consist of the individuals listed in Appendix A, having the noted roles and responsibilities. This team will have both primary members and secondary members. The primary members of the IRT will act as first responders or informed members to an

incident that warrants IRT involvement, according to the incident's severity. The entire IRT would be informed and involved in the most severe incidents.

IRT members may take on additional roles during an incident, as needed. Contact information, including a primary and secondary email address, plus office and mobile telephone numbers, shall be maintained and circulated to the team. The IRT will draw upon additional staff, consultants or other resources, (often referred to as Subject Matter Experts – SME's) as needed, for the analysis, remediation, and recovery processes of an incident. The Information Technology (IT) function plays a significant role in the technical details that may be involved in incident detection and response and can be considered an SME in that regard.

There shall be a member of the IRT designated as the Incident Response Manager (IRM), who will take on organizational and coordination roles of the IRT during an incident where the IRT is activated for response to the incident.

Incident Response Life Cycle Process

Cyber incident response management is an on-going process with a cyclical pattern. The specific incident response process elements that comprise the Cyber Incident Response Plan include:

1. **Preparation:** The on-going process of maintaining and improving incident response capabilities and preventing incidents by ensuring that systems, networks, applications, and data handling processes are sufficiently secure, and employee awareness training is in place. Practice exercises (aka Table-top Exercises) for the IRT are conducted annually, where various incident scenarios are presented to the Team in a practice session.
2. **Identification:** The process of confirming, characterizing, classifying, categorizing, scoping, and prioritizing suspected incidents.
3. **Notification:** Alerting IRT members to the occurrence of an incident and communicating throughout the incident.
4. **Containment:** Minimizing financial and/or reputational loss, theft of information, or service disruption. Initial communication with constituents and news media, as required.
5. **Eradication:** Eliminating the threat.
6. **Recovery:** Restoring computing services to a normal state of operation and the resumption of business activities quickly and securely. Provide reputational repair measures and news media updates, if needed. Provide credit monitoring services to affected constituents, or other remediation measures, as

appropriate.

7. **Post-incident Activities:** Assessing the overall response effectiveness and identifying opportunities for improvement through, 'lessons learned' or mitigation of exploited weaknesses. Incorporation of incident's learnings into the cyber fortification efforts and the response plan, as appropriate.

Incident Occurrence & Awareness

The way an incident becomes known will have an impact on the response process and its urgency. Examples by which Capita and/or IT become aware of an incident include, but are not limited to the following:

1. Capita and/or IT discovers through its internal monitoring that a cyber incident or data breach has occurred.
2. Capita is notified by one of its technology providers of an incident or becomes aware of the same.
3. Capita is made aware of a breach through a constituent or a third-party informant.
4. Capita and the public are made aware of the incident through the news media.

Incident Response Process Detail

The response process, at a detail level, for an incident includes 5 of the 6 life cycle phases, as it excludes the Preparation phase. The detailed steps and general timing of an incident response are outlined below. The IT function is specifically called out as an involved party, separate from other SMEs.

Process Phase & Approximate Timing	Process Detail Steps	Involved Parties
Identification (Hours)	1. Identify and confirm that the suspected or reported incident has happened and whether malicious activity is still underway. 2. Determine the type, impact, and severity of the incident by referring to **Appendices B, C, and D**. 3. Take basic and prudent containment steps.	The IRM, IT, and any monitoring service provider

Notification (Hours – 1 Day)	4. Inform or activate the IRT, based on the severity of the incident, as outlined in **Appendix D**, and provide the type, impact, and details of the incident to the extent that they are known. 5. IRM, or delegate, fills out **Appendix E** accordingly. 6. Determine the need for Subject Matter Experts (SME) to be involved in the Containment, Eradication, and Recovery processes.	IRM, IT, & IRT
Containment (Hours-2 Days)	7. Take immediate steps to curtail any on-going malicious activity or prevent repetition of past malicious activity. 8. Re-direct public facing websites, if needed. Provide initial public relations and legal responses as required.	IRT, IT, SME's
Eradication (Days -Weeks)	9. Provide full technical resolution of threat and related malicious activity. 10. Address public relations, notification, and legal issues. 11. (Per SEC Regulation S-P Policy, must notify required parties within 72 hours)	IT, IRT, SME's
Recovery (Weeks -Months)	12. Recover any business process disruptions and re-gain normal operations. 13. Address longer term public relations or legal issues, if required, and apply any constituent remedies. 14. (Per SEC Regulation S-P Policy, must notify required parties within 30 days)	SME's, IRT
Post-incident (Months)	15. Formalize documentation of incident and summarize learnings. 16. Apply learnings to future preparedness. 17. Schedule after-action review of incident based on severity.	IRT

Communication Methods

Company communication resources (email, phone system, etc.) may be compromised during a severe incident. Primary and alternate methods of communication using external

infrastructure will be established and noted on the IRT member contact list to provide specific methods of communication during an incident. The IRT and any other individuals involved in an incident resolution will be directed as to which communication method will be used during the incident.

Information Recording

Information recording is very important during an incident, not only for effective containment and eradication efforts, but also for post-incident lessons learned, as well as any legal action that may ensue against the perpetrators. The IRM, or delegate, shall be responsible for recording information and chronological references about their actions and findings during an incident, using the IRT Incident Record Form in Appendix E. All information and documentation shall be maintained and preserved in accordance with regulatory requirements, for a period of no less than five years.

Incident Response Exercises

The IRT should conduct 'table-top' exercises to practice the response process on a periodic basis, but at least annually, so all members of the IRT are familiar with the activities that would occur during an actual incident and their related responsibilities. The exercises may provide the opportunity for enhancing the coordination and communication among team members.

Summary

No perfect script can be written for the detailed activity encountered and decisions that will need to be made during an incident, as each incident will have its own uniqueness. This plan shall serve as a framework for managing cyber security and data breach incidents, allowing the details of confirmation, containment, eradication, and communication to be tailored to fit the specific situation.

This policy shall be reviewed annually by executive leadership and updated as needed. The policy shall be signed by the President or equivalent officer upon each review.

Appendix A

Team Members and Roles

Primary Team Members

Incident Response Manager (IRM) Scott Watko

Communication Methods

- Primary email address: scott@capitamail.com
- Secondary email address: Ironmanscott67@gmail.com
- Primary phone (cell): 801-641-7459
- Ring Central phone: 385-498-5841

Responsibilities

- Coordinate communications and activities of the IRT when it is activated
- Maintain proactive cybersecurity policies and procedures
- Notify IRT members of incidents and provide updated

Technology Liaison Rylie Reynolds

Communication Methods

- Primary email address: rylie@capitamail.com
- Secondary email address: rylie.mcclellan@gmail.com
- Primary phone (cell): 801-870-8403
- Ring Central phone: 385-498-5781

Responsibilities

- Discover and/or verify cyber incidents
- Coordinate computer forensic and technical remediation activities
- Apply corrective actions to technology infrastructure

Executive level manager in charge of financial management Cassie Myers

Communication Methods

- Primary email address: cassie@capitamail.com
- Secondary email address: cassiecmyers@gmail.com
- Primary phone (cell): 801-580-8162
- Ring Central phone: 801-623-6604

Responsibilities

- Financial impact and financial data exposure

Executive level manager in charge of external communications and public relations Zacc Call or Mike Littledike

Communication Methods

- Primary email address: zacc@capitamail.com or mike@capitamail.com
- Secondary email address: zacccall@gmail.com or mlittledike@gmail.com
- Primary phone (cell): 801-824-0734 or 801-889-8380
- Ring Central phone: 801-854-7346 or 801-616-3710

Responsibilities

- Public relations
- News media management
- External and internal communication

Executive level manager in charge of human resources Cassie Myers

Communication Methods

- Primary email address: cassie@capitamail.com
- Secondary email address: cassiecmyers@gmail.com
- Primary phone (cell): 801-580-8162
- Ring Central phone: 801-623-6604

Responsibilities

- Communication to employees
- Employee data exposure issues

Executive level manager in charge of company operations Cassie Myers

Communication Methods

- Primary email address: cassie@capitamail.com
- Secondary email address: cassiecmyers@gmail.com
- Primary phone (cell): 801-580-8162
- Ring Central phone: 801-623-6604

Responsibilities

- Operational impact and/or overall data exposure assessment

Executive level manager in charge of physical security Cassie Myers

Communication Methods

- Primary email address: cassie@capitamail.com
- Secondary email address: cassiecmyers@gmail.com
- Primary phone (cell): 801-580-8162
- Ring Central phone: 801-623-6604

Responsibilities

- Building access and control

Secondary Team Members

Security event monitoring vendor and/or computer forensics vendor Equinox IT (Tyson Bottorff)

Communication Methods

- Primary email address: tysonb@equinoxits.com
- Secondary email address: tam@equinoxits.com
- Primary phone (cell): 801-822-8233
- Work phone: 801-426-7800

Responsibilities

- Detection
- Mitigation
- Technical Forensics

Legal representative Michael Best & Friedrich LLP (Betsy Voter)

Communication Methods

- Primary email address: btvoter@michaelbest.com
- Primary phone (cell):
- Work phone: 801-924-4105

Responsibilities

- Legal Advisor
- Contractual matters

Cyber insurance provider Golsan Scruggs (Cameron Norris) Carrier is Markell

Communication Methods

- Primary email address: cnorris@golsanscruggs.com
- Primary phone (cell):
- Work phone: 503-244-0297 X107

Responsibilities

- Cyber Insurance advisor
- Contact information and communication methods for the IRT members should be distributed to the team separately as confidential information.

Appendix B – Incident Categorization

Common Categories Of Cyber Incidents

Incident Type	Type Description
Unauthorized Access	When an individual or entity gains logical or physical access without permission to a company network, system, application, data, or other resource.
Denial of Service (DoS, DDoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
Malicious Code	Successful installation of malicious software (e.g., a virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.
Improper or Inappropriate Usage	When a person violates acceptable computing policies, including unauthorized access or data theft.
Suspected PII Breach	An incident where it is suspected that Personally Identifiable Information (PII) has been accessed.
Suspected loss of Sensitive Information	An incident that involves a suspected loss of sensitive information (not PII) that occurred because of Unauthorized Access, Malicious Code, or Improper (or Inappropriate) use, where the cause or extent is not known.

Appendix C – Incident Impact Definitions

Security Objective	General Description	Potential Impact Examples		
		Low	Medium	High
Confidentiality: *Preserving restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*	The unauthorized disclosure of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Limited to a single or several Users or computers in an isolated fashion, with easy remediation	Involving or affecting a group of Users, resulting in access to proprietary information. Limited or no external exposure.	A severe breach of proprietary information with external exposure.
Integrity: *Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.*	The unauthorized modification or destruction of information could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Inadvertent or non-malicious alteration or deletion of company data that is easily remediated.	An on-going improper data alteration act (or series of acts) of malicious or negligent nature that will have a moderate business impact.	A massive alteration or destruction of company data of a malicious or obstructive nature.
Availability: *Ensuring timely and reliable access to and use of information systems.*	The disruption of access to or use of information or an information system could be expected to have the following adverse effect on organizational operations, organizational assets, or individuals.	Isolated outage or inaccessibility affecting a limited number of Users for a short amount of time (< 2 hours)	A widespread outage or inaccessibility of a primary business system lasting more than 2 hours, but less than a day	Severe outage or inaccessibility of the company business systems lasting a day or more.

Appendix D – IRT Incident Severity & Response Classification Matrix

Severity Level (5=Most Severe)	Typical Incident Characteristics	Example of Impact	Incident Response	Activate IRT?
5	DDoS attack against on-premise or hosted Servers. Active attacks against network infrastructure. Access to internal company data by nefarious parties.	An enterprise-wide attack involving multiple departments that prevents access to systems and disrupts business operations. Access to or theft of proprietary data.	IRT and the IRM direct response. Remediation coordinated by IT, Forensics, and SMEs. Possible Legal Counsel, Law Enforcement involvement	Full Team Active
4	Affects data or services for a group of individuals and threatens sensitive data, or involves accounts with elevated privileges with potential threat to sensitive data	Compromised business application. Improper or unauthorized access to data.	Response coordinated by IRM, IT, and SME's; IRT advised. Legal Counsel specifically notified if there is a PII breach.	Full Team Informed and Advised
3	Affects data or services of a single individual, but involves significant amounts of sensitive data, may include PII.	Employee computer or account with sensitive data access compromised; physical theft of device, unprotected media, or hard copy data.	Response coordinated by IT or IRM, with information sent to the IRT members. Legal Counsel notified if a PII breach	Primary Team Informed
2	Affects data or services of a group of individuals with no sensitive data involved.	Compromise of an account or device with shared folder access.	Response coordinated by IT. IRM advised and IRT informed. IT documentation process used to record findings.	Primary Team Informed
1	Affects data or services of a single individual with no sensitive data beyond them; focus is on correction and future prevention	Compromised computer with no sensitive data etc.	Documentation of issue and findings. Response/remediation coordinated by IT, IRM advised of the incident.	No
0	Occurrences of very minor or undetermined focus, origin and/or effect for which there is no practical follow-up	Impaired computer requiring review of system access logs, AV scans, or other repairs.	Documentation through normal IT support processes to record actions and resolution. Reset passwords as needed.	No

Appendix E – IRT Incident Record Form

Incident:

Discovery Date:

Recorded By:

Recorded Information and Events

Date & Time:

Details

Cyber and Data Security Incident Response Plan Document Version History

Version	Date	Changes/Notations
1.0	July 1, 2025	Initial release

Business Continuity & IT Security Manual Version History

Business Continuity & IT Security Manual Version History

Version	Date	Changes/Notations
1.0	November 2025	Initial release