Cyber Security & Information Security Policy

CAI has appointed Scott J Zollo as the firm's Chief Information Security Officer ("CISO"). The CISO is responsible for managing CAI's information security program.

Access Persons

Access Person: Any of CAI's supervised persons who have access to non-public information regarding any client's purchase or sale of securities, or information regarding the portfolio holdings of any reportable fund, or who is involved in making securities recommendations to clients, or who has access to such recommendations that are non-public.

The following employee(s) will manage non-public information:

Name	Title
Scott J Zollo	President

The following individual(s) also have access to non-public information:

Name	Title
Sean Collins	Vice President
Terrance Collins	Vice President
Robert Brown Jr.	Senior Associates

Inventory of Technology Infrastructure

On an annual basis, the CCO of CAI will make an inventory of the following:

- Physical devices and systems (computers, servers, etc.);
- Software platforms and applications (email applications, file management, etc.);
- Systems that house client data; and
- Third-party contractors that have access to systems, platforms, etc.

CAI's primary software platforms that may contain client data are summarized below.

Type of System	Name of System
Customer Relationship Management (CRM)	Advisors Assistant
Email Provider / Hosting	BlueTie
Financial Planning	Money Guide Pro
Email / Social Media Archiving	Bluetie for email.
Document Management / Storage	ReadyDoc

Type of System	Name of System
Reporting / Portfolio Management	Morningstar

CAI utilizes cloud-based technology systems, which it believes provide increased information security capabilities including:

- Ability to leverage the established infrastructure of trusted technology industry leaders; and
- Improved system alert capabilities including better user activity logging and alerts related to unusual user activity.

CAI also recognizes that cloud-based technology creates a greater reliance on passwords and user login security. In particular, CAI understands that certain users with administrative access to the firm's cloud-based technology systems may pose even greater risk given their expanded access to sensitive client data. As such, CAI has designed and will continue to further develop information security policies with this increased risk as a focus.

Security of Technology Infrastructure

CAI has implemented the following firm-wide information security polices to help prevent unauthorized access to sensitive client data:

- All computers used to access client data will have antivirus software installed. In addition, the antivirus software will have an active subscription and all updates will be scheduled to automatically install.
- All staff will utilize devices with up to date operating system software with all security patch and other software updates set to automatically install
- All staff workstations (e.g. desktop, laptop, mobile device) will be locked when the device is not in use
- All staff workstations (e.g. desktop, laptop, mobile device) will be shut down completely at the end of each workday
- All staff workstations (e.g. desktop, laptop, mobile device) will use proper data encryption when possible
- All staff mobile devices used to access work email and files will be password protected and will have the capability to be remotely wiped if lost or stolen
- All staff members are prohibited from accessing CAI systems from unsecured internet connections

All staff should immediately alert the CCO of any suspicious behavior or potential incidents.

Detection of Unauthorized Activity or Security Breaches

The CCO is responsible for monitoring on-site and cloud-based systems for suspicious activity and security breaches. Such unauthorized activity or security breaches may include:

- Logins to company systems after traditional business hours for the local region
- Logins to company systems from non-local regions (e.g. outside of the local region, the United States, etc.)
- Large transfers of files or data

When suspicious activity or a potential security breach is discovered, the CCO will restrict access to the systems and begin to assess what information may have been accessed and what actions need to be taken to remediate the event.

Regardless of the severity, the CCO will keep a log of all incidents and note the action taken. This log will include the following information about each incident:

- Date and time of the incident
- How the incident was detected
- The nature and severity of the incident
- The response taken to address the incident
- Any changes made to the Cyber Security & Information Security Policy as a result of the incident

In addition, all staff should immediately alert the CCO of any suspicious behavior or concern.

If the incident is deemed by the CCO to have led to unauthorized release or use of sensitive client information, then the CCO will take the following steps:

1) Communicate the details of the event to the relevant principals of the firm
2) Determine if any staff disciplinary action needs to be taken
3) Determine if any third party vendors were involved in the incident
4) Contact proper law enforcement and/or regulatory agencies as required by law (if necessary)
5) Communicate the details of the event and steps being taken to rectify the incident to impacted clients of the firm (if necessary)

Prevention of Unauthorized Funds Transfers

CAI has implemented the following firm-wide information security polices to help prevent unauthorized funds transfers:

- Clients must confirm all third party wire requests verbally. Wire requests may not be authorized solely via email; and
- Wire requests should be reviewed for suspicious behavior (e.g. time of request, atypical amount of request, etc.).

CAI is particularly aware of the risk caused by fraudulent emails, purportedly from clients, seeking to direct transfers of customer funds or securities and will train staff members to properly identify such fraudulent emails.

User Login Security

CAI has implemented the following firm-wide user login security polices to help prevent unauthorized access to sensitive client data:

- All staff passwords are required to meet or exceed the following guidelines:
  - Contain both upper and lower case letters
  - Contain at least one number
  - Contain at least one special character
  - Be at least 10 characters in length
  - May not contain words that can be found in a dictionary
  - May not contain personal information such as pet names, birthdates, or phone numbers
- All staff are required to have unique passwords to access each technology system (e.g., desktop computer, CRM system, etc.)
- All staff are required to update passwords on a quarterly basis
- No passwords are allowed to be stored in writing on paper or on any system
- Staff members should not use the "remember password" feature of any application
- Staff members should never share passwords with any other staff member or third party
- When available, staff is required to utilize two-factor authentication

In addition, all staff members should never disclose personal information on any social media website that could allow a third party to gain access to CAI's systems. Such information includes but is not limited to:

- Birthdate
- Place of birth
- Place of wedding
- Name of high school
- Name of elementary school
- Best friend's name
- Name of favorite pet
- Name of favorite drink
- Name of favorite song
- Mother's maiden name
- Make and model of first car
- Favorite color
- Name of favorite teacher

User Access Privileges

CAI has implemented the following firm-wide user access privilege polices to help prevent unauthorized access to sensitive client data:

- All new staff members login credentials will be created by the CCO;
- Staff members will only have access to systems deemed necessary by the CCO;
- Staff members, besides the CCO or other designated personnel, will not have access to administrative privileges on systems unless deemed necessary by the CCO; and
- Upon a staff member's departure or termination, the CCO will immediately remove the former staff member's access to all firm systems.

Staff members may request additional access to systems by contacting the CCO.

Email Use Security and Guidelines

CAI has implemented the following firm-wide email use security polices and guidelines to help prevent unauthorized access to sensitive client data:

- All staff should only provide sensitive information electronically to clients via a secure email or client portal;
- All staff should never open or download any email attachments from unknown senders;
- All staff should never open or download any email attachments from known senders that look suspicious or out of the ordinary;
- All staff should never directly click on or open any links sent in emails; and
- All staff should be acutely aware of any attempted "phishing" emails seeking to obtain the staff member's user login credentials. Some warning signs to look for include:
    - Bad spelling or poor grammar in the email subject or body text;
    - A company or website with which the staff member is not familiar; and
    - A suspicious sender email domain.

When a staff member receives a suspicious email, the CCO should be immediately alerted. The CCO will then determine next steps and communicate to other staff members if deemed appropriate.

Mobile Device Usage Guidelines

In order to help prevent unauthorized access to sensitive client and firm data, CAI permits the limited use of personal mobile devices only under the following firm-wide mobile device usage guidelines:

- Before utilizing a personal mobile device to access company systems such as company email, the device must be inspected and approved by the CCO to ensure proper security features are activated on the device.
- The mobile device's built-in password / passcode security feature must be activated at all times.
- If available, the mobile device's local or remote wipe security features(s) should be activated.
- Staff members should take great caution to not use the mobile device in public places that could expose sensitive client or firm information.

- In the event a mobile device used to access company systems is lost or stolen, the staff member should immediately alert the CCO.
- Before disposing of any mobile device used to access company systems, all data must be wiped from the mobile device.

Sensitive client or firm information should never be stored or downloaded onto a personal mobile device. If the staff member's mobile device does not offer a built-in password / passcode security feature, then the device is not permitted to be used to access company systems.

Third Party Vendor Security and Diligence

CAI has implemented the following firm-wide third party vendor security and diligence polices and guidelines to help prevent unauthorized access to sensitive client data:

- All third party vendors that have physical access to the office and/or the firm's systems are required to enter into a non-disclosure agreement (NDA) in order to protect sensitive client information before establishing a business relationship; and
- Proper due diligence will be performed on all relevant technology vendors prior to establishing a business relationship and then again on at least an annual basis and will include:
    - Review of the firm's information security policies;
    - Review of the firm's disaster recovery policies; and
    - Review of the firm's general capabilities to ensure it meets CAI's needs.

All of this information will be stored and maintained in CAI's vendor diligence file.

Significant Technology System Disruption Plan

In the event of a significant business disruption that results in a significant interruption in access to the firm's technology systems; CAI will implement its business continuity plan as detailed in this policies and procedures manual.

In the event of the theft, loss, unauthorized exposure, or unauthorized use or of access of client information, the incident will be investigated and documented by the CCO. In the event of a technology system breach, CAI will comply with all local and federal laws to communicate accordingly with the affected third parties.

Testing

On a quarterly basis, CAI will test its current Cyber Security & Information Security Policy and capabilities. The test conducted by the CCO will include the following activities:

- Ensure all staff members have proper system access privileges;
- Ensure all relevant software patches designed to address security vulnerabilities have been implemented on the firm's internal server; and

- Make a physical inspection of the office to ensure that all workstations have the proper security measures including:
    - Attempt to access a random sample of firm devices to ensure that proper passwords are in place to prevent access;
    - Observe staff members access systems with the proper password to ensure that two-factor authentication has been activated;
    - Ensure staff members are not using the "remember password" feature of any application;
    - Ensure computers used to access client data have an antivirus software subscription; and
    - Ensure no passwords are visibly stored in writing on paper or on any system.

On an annual basis, CAI will further test its current Cyber Security & Information Security Policy and capabilities. The test conducted by the CCO will include the following activities:

- Conduct a risk assessment to determine if any changes need to made to information security policies and procedures;
- Attempt to access users' accounts with the proper password to ensure that two-factor authentication prevents system access;
- Perform any relevant third party penetration tests or vulnerability scans and remediate any relevant discoveries; and
- Attempt to restore a sample of files and records from the systems inventoried above to ensure that the restoration process is sufficient and properly configured.

The results from the annual test will be documented and utilized as an opportunity to update the Cyber Security & Information Security Policy.

Data Back-Up Policies

CAI stores sensitive firm and client data on local and third party systems as documented in CAI's *Inventory of Technology Infrastructure*. This data is backed up in accordance with CAI's data back-up and recovery procedures.

Staff Training

On an annual basis, CAI will conduct a firm-wide training session to ensure that all staff members are properly trained and equipped to implement the above policies. New staff members will receive training, led by the CCO, within one (1) month of their initial hire date. The training conducted by the CCO will include the following topics:

- Review of the current Cyber Security & Information Security Policy, including a note of any changes to the policy since the last training session;
- Review of any relevant information security incidents or suspicious activity;
- Review of how to identify potential "phishing" or fraudulent emails;
- Review of how to identify potential "Ransomware" or similar attacks;
- Review of any relevant regulatory compliance changes or developments; and

- Review of general information security best practices.

Chief Compliance Officer Appointment

The person herein named "Chief Compliance Officer" is stated to be competent and knowledgeable regarding the Advisers Act or applicable state rule or regulation and is empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the firm. The compliance officer has a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

Chief Compliance Officer	Date Responsibility Assumed	Annual Review Completed
Scott J Zollo	1/1/2006	4/16/2021