Bay Colony Advisory Group, Inc d/b/a Bay Colony Advisors

Cybersecurity Policy

Effective date: August 15, 2017

This Cybersecurity Policy is the property of Bay Colony Advisory Group, Inc d/b/a Bay Colony Advisors and its contents are confidential unless approved by the Chief Compliance Officer.

Bay Colony Advisory Group, Inc d/b/a Bay Colony Advisors
86 Baker Avenue Extension
Suite 310
Concord, MA 01742
Phone: (978) 369-7200 * Fax: (617) 249-1807

1. Cybersecurity Policy Objectives and Scope

Objective
Bay Colony Advisory Group, Inc d/b/a Bay Colony Advisors ("BCA" or the "Advisor") has adopted this Cybersecurity Policy ("Policy") to provide guidance to BCA employees, contractors and those subject to BCA's compliance program (collectively "Supervised Persons") for the storage or transmission of confidential digital information. It is the objective of this Policy to describe the safeguards and procedures for ensuring that information entrusted to BCA by its clients is not acquired or transmitted by any unauthorized individual or entity. This Policy is also intended to address suspected privacy policy breaches pursuant to Regulation S-P in addition to identity theft red flags and how those red flags are addressed pursuant to Regulation S-ID.

Scope
This Policy applies to all Supervised Persons of BCA and any digital storage device or medium that is under the control or ownership of BCA or otherwise authorized to, or is intended to, store personal information about a client of BCA.

Responsibility
BCA has assigned the Advisor's Chief Compliance Officer ("CCO") as the individual with primary responsibility for implementing and revising this Policy ("Responsible Person"). The Responsible Person may delegate all or a portion of these responsibilities to a delegate of their choice, so long as that delegate is an employee of the Advisor or a third-party entity that is reasonably capable of implementing this Policy.

2. Definitions
The following definitions are used within the regulation and are provided here for clarification:

Breach of security: the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a person. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

Cybersecurity: the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

Electronic: relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted: the transformation of data into a form in which meaning of the original data cannot be observed without the use of a confidential process or key to reverse the transformation.

Identity Theft: When a person assumes the identity of another in order to generate fraudulent transactions or other harmful conduct that impacts the assumed person to the benefit of the person initiating the transaction or conduct.

Owns or licenses: receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person: a natural person, corporation, association, partnership or other legal entity.

Personal information: a client's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such client: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a client's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record(s): any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider: any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to this regulation.

Suspicious Activity: activity that is indicative of fraudulent or illegal activity, or involves transactions that are not typical with a particular client, such as sudden requests to withdraw large sums.

3. Potential Cybersecurity Sources

Internal

A source of potential cybersecurity vulnerabilities is from the conduct of Supervised Persons of BCA. Whether intentional or accidental, private information about the client may be revealed or sent to someone outside the firm in a manner that exposes it to unreasonable cybersecurity threats and potentially discloses the information to the public. Internal Cybersecurity sources may include but are not limited to:

- Sending sensitive data to wrong recipient – If you fail to review the recipients before sending sensitive data, having selected a recipient unintentionally.
- Not using encryption to send private data – If you to send private data without using secure message procedures, such as encryption.
- Sharing credentials for account access – If you share credentials with any other individual, the Advisor loses the ability to have an audit trail in their system access logs and the individual may further share the credentials or otherwise cause a breach of security.
- Account access not updated – Not reviewing and updating the access of accounts used by Supervised Persons can lead to breaches in security if the Advisor is seeking to implement an access hierarchy.
- Securing the facility – If the Advisor's offices are not secure when unoccupied, it can lead to a breach in security.
- Keeping systems updated – If the applications and anti-virus software is not kept up to date it can lead to security vulnerabilites that are more easily exploited and thus a breach of security.
- Use complex passwords – It is generally accepted that certain passwords are more vulnerable to others based upon the complexity of the characters used.

External

Cybersecurity vulnerabilities can also arise from external sources, such as messages received by Supervised Persons or persons unrelated to the Advisor seeking to gain access to the Advisor's private information for further attacks or violations. It is critical for any knowledge of external cybersecurity vulnerabilities, or perceived breaches of the Advisor's network or information security controls to be escalated to the Responsible Person. External Cybersecurity sources may include but are not limited to:

- Clients – Clients may send files that have viruses in the normal course of providing requested information.
- Vendors and Third-Parties – Similar to Clients, files and emails must be scanned for viruses by Supervised Persons.
- Suspicious activity – Client email accounts may be accessed by an unauthorized individual or otherwise hacked, such that they attempt to transmit viruses to the account's contacts, upload malicious software, or seek to exploit the relationship with the Advisor by requesting funds.
- Identity theft – A prospect, or someone acting as a client, may try to create an account with a false identity in order to gain physical access to the Advisor's office, or an expectation of sending files that would be intentionally infected with a virus.

4. Controls to Address Cybesecurity Sources

The Advisor has implemented the following controls to address the sources of cybersecurity vulnerabilities as described in section 3 above. These controls seek to reasonably minimize any harm to the Advisor, its Supervised Persons and its clients, in response to a cybersecurity threat or attack.

Internal

- Sending sensitive data to wrong recipient – Supervised Persons are expected to review the recipients before sending sensitive data.
- Email disclosures and footers – Supervised Persons that communicate using the Advisor's email domain will include a footer in their email signature that, should it be sent to an unintended recipient, be promptly deleted and not forwarded.
- Transmitting sensitive data – All files containing private client data will be sent using encryption or by means of another secure delivery process. At no time will private client data be sent over public networks in plain text (unencrypted) or otherwise published online on a public site.
- Storing sensitive data – All files containing personal information of clients that will be kept in the Advisor's possession will be stored using encryption on the disk they are stored, or using a password-protected machine to ensure access only by authorized individuals. At no time will a device store private client data without being protected by encryption or a password to access such data.
- Credentials not shared – Supervised Persons are prohibited from sharing account credentials with any other person without the consent of the Responsible Person. Passwords must be kept private.
- Account credential review – The Responsible Person will review account credentials of systems used by Supervised Persons at least annually and update as needed to ensure access to the Advisor's systems by Supervised Persons is appropriate.
- Secure facility – The Advisor's offices will be locked when unoccupied.
- Updating systems – The Responsible Person will review, at least quarterly, the status of applications, including anti-virus programs, to ensure that all available security updates are installed.
- Training – This Policy will be included in the Advisor's annual compliance training agenda and Supervised Persons will be able to ask questions about the implementation of this Policy.
- Periodic risk assessments – An element of the Advisor's compliance program includes an annual assessment of its policies and procedures, including this Policy. The risk assessments will be kept with the Advisor's books and records for at least five (5) years from the date of completion.
- Data backup – The Advisor's critical data will be backed up as detailed in their Business Continuity Plan.

- Reporting concerns or violations – Supervised Persons are required to report any observed or suspected violations to the Responsible Person promptly and no later than end of the business day when it was first observed.
- Secure destruction – Any personal information will be securely destroyed to ensure that the personal information cannot be accessed by subsequent persons in possession of the disk or resource being destroyed by the Advisor.

External

- Scan for viruses – All files received, including email attachments or physical disks, from clients and vendors must be scanned for viruses.
- Remote access – All personal information of clients will be accessed remotely through an encrypted connection to the other computer before viewing or transmitting any personal information of clients. All personal information of clients is to be transmitted as described above under "Transmitting sensitive data".
- Updating systems – The Responsible Person will review, at least quarterly, the status of both hardware and software applications, including anti-virus programs and firewalls, to ensure that all available security updates are installed.
- Suspicious activity – Supervised Persons are required to report any actual or potential suspicious activity observed to the Responsible Person promptly and no later than end of the business day when it was first observed. This includes any suspicion of identity theft involving clients or other Supervised Persons.

5. Responding to a Cybersecurity Attack

The response to a cybersecurity attack will be reasonably related to the nature of the attack. Should a Supervised Person suspect their computer, device, or network has been subjected to a breach of security, they will promptly notify the Responsible Person and provide any requested details to determine the nature of the breach of security and the extent of the cybersecurity attack. The Responsible Person will document all related information, the results of analyzing such information, and any response to address the suspected or actual breach of security.

Appropriate responses may include, but are not limited to, monitoring client account(s), contacting the client, changing security settings, changing the Advisor's policies and procedures, closing the account(s), and/or notifying custodian(s) and law enforcement.

6. Testing the Cybersecurity Policy

BCA shall review this Policy and test its effectiveness at least annually. The Responsible Person shall document the findings of the testing in a report to be kept with the Advisor's books and records.

Annually, BCA shall also request or review available information from its vendors that store or handle client personal information to ensure they maintain a reasonably adequate cybersecurity policy to support the activities of BCA. Any deficiencies will be addressed with the service provider and documented in a report to be kept with the Advisor's books and records and/or the annual CCO report of the effectiveness of the Compliance Program.

7. Updating the Cybersecurity Policy

BCA may make periodic updates to this Policy to account for changes in business practices, regulations and best practices. If any material changes are made to the Policy, all BCA Supervised Persons shall receive a copy and be expected to certify their understanding of the plan.