Acts Financial Advisors

Cybersecurity Policy

Effective Date: May 10, 2023

TABLE OF CONTENTS

POLICY STATEMENT

Acts Financial Advisors ("Adviser") acknowledges that Cybersecurity is a significant risk, and this section of the manual memorializes the policies, procedures and controls Adviser has implemented to address cyber threats.

At a minimum, Adviser will annually review and assess the design and effectiveness of the cybersecurity policies and procedures required, including whether they reflect changes in cybersecurity risk over the time covered by the review. Adviser will prepare a written report that describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.

DEFINITIONS

- ***Adviser information*** means any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.
- ***Adviser information*** systems means the information resources owned or used by the adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.
- ***Cybersecurity incident*** means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.
- ***Cybersecurity risk*** means financial, operational, legal, reputational, and other consequences that could result from cybersecurity incidents, threats, and vulnerabilities.
- ***Cybersecurity threat*** means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.
- ***Cybersecurity vulnerability*** means a vulnerability in an adviser's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.
- ***Personal information*** means any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information; or any other non-public information regarding a client's account.
- ***Significant adviser cybersecurity incident*** means a cybersecurity incident, or a group of related cybersecurity incidents, that significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in substantial harm to the adviser, substantial harm to a client, or an investor in a private fund, whose information was accessed.

CYBERSECURITY COORDINATOR DESIGNATION

We have designated [CCO Full Name] to implement, supervise and maintain the Program. That designated employee (the "Cybersecurity Coordinator") will be responsible for:

- Initial implementation of the Program.
- Training employees.
- Regular testing of the Program's safeguards.
- Evaluating the ability of each of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access and requiring such third-party service providers by contract to implement and maintain appropriate security measures.
- Reviewing the scope of the security measures in the Program at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.

- Conducting an annual training session for all relevant staff, including temporary and contract employees who have access to personal information on the elements of the Program. All attendees at such training sessions are required to certify their attendance at the training and their familiarity with the Adviser's requirements for ensuring the protection of personal information.

The written policies and procedures below are intended to satisfy the requirement of Rule 206(4)-9 or corresponding State Regulatory Jurisdictions as applicable.

CYBERSECURITY WRITTEN POLICIES AND PROCEDURES

New Rule 206(4)-9 requires cybersecurity policies and procedures. As a means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the Act (15 U.S.C. 80b6(4)), it is unlawful for any investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3) to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks.

Risk Assessment

Adviser must perform periodic assessments of cybersecurity risks associated with adviser information systems and adviser information residing therein, including requiring the adviser to:

- Categorize and prioritize cybersecurity risks based on an inventory of the components of the adviser information systems and adviser information residing therein and the potential effect of a cybersecurity incident on the adviser; and
- Identify the adviser's service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein, and assess the cybersecurity risks associated with the adviser's use of these service providers.
- Require written documentation of any risk assessments.
- Adviser will maintain documentation of all cybersecurity risk assessments and remedial steps taken.

*Adviser may, if determined necessary by the Chief Compliance Officer, acquire the services of a third-party Cybersecurity vendor to assist in conducting risk assessments. Documentation of this

User Security and Access

The Adviser must implement controls designed to minimize user-related risks and prevent unauthorized access to adviser information systems and adviser information residing therein, including:

- Requiring standards of behavior for individuals authorized to access adviser information systems and any adviser information residing therein, such as an acceptable use policy (see below).
- Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification.
- Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication.
- Restricting access to specific adviser information systems or components thereof and adviser information residing therein solely to individuals requiring access to such systems and

information as is necessary for them to perform their responsibilities and functions on behalf of the adviser; and
- Securing remote access technologies.

Acceptable Use Policies

Supervised Persons must:

- Take reasonable precautions to protect Adviser's systems and data.
- Access files, data, and protected records only if you are authorized do to so or if the information is publicly available.
- Contact IT if there is doubt concerning your authorization to access any Adviser IT resource.
- Take care to protect passwords that are used to access the firm's systems.
- Be vigilant to potential phishing attacks:
- Take reasonable steps to confirm the identity of any client or other authorized person requesting client nonpublic information before providing such information; and
- Take reasonable steps to confirm the identity of individuals and the security or authenticity of any websites before providing company confidential information, including but not limited to, account numbers and passwords.
- Guard against access to files and take precautions to protect Information Technology (IT) devices when you are away from the workstation, including logging off or locking computers or other devices.
- Only use software furnished by the Adviser. Under certain circumstances, you may use the software if it has first been approved by IT and/or the third-party IT provider.
- Contact the CCO or other authorized person if you need to transfer data from Adviser's system.

MOBILE DEVICES AND EXTERNAL STORAGE

When using an external storage media or another device to transfer data:

- The device used must be an Adviser-approved device.
- Employee purchased media, or those containing personal information, must not be connected to Adviser equipment at any time.
- External media must be encrypted, and password protected.
- Employees should not store Adviser business-related data on external media. All Adviser business-related data must be stored on the company's network drive.
- If Adviser network connection is unavailable (ex: training outside of Adviser), external media may be used for short-term data storage and backup purposes only if approved by Adviser.

Password Protection

- Passwords are said to be the "weakest link" of cybersecurity. Multi-factor authentication (MFA) requires at least two forms of authentication such as a security token in addition to the username and password. The three critical use cases for MFA are securing computer logins, the file server, and email accounts. The adviser will attempt to implement MFA whenever possible.
- Remote access to the Adviser network must be secured via a VPN (Virtual Private Network) and MFA.

- When MFA is not available, the Adviser will implement password creation guidelines and store passwords securely, only using systems designed to protect passwords with sufficient encryption.
- Upon termination of personnel, IT will immediately change any passwords that could be used to access firm systems or client accounts on a remote basis. This includes individual as well as firm-wide passwords.
- Adviser recommends that passwords include at least 12 characters and three of the following: number, lower case letter, upper case letter, or symbol.
- Supervised persons are to update or reset passwords at least once every six months and are instructed to refrain from sharing passwords outside of a firm-authorized password sharing system.

INFORMATION PROTECTION

- Adviser must implement measures designed to monitor adviser information systems and protect adviser information from unauthorized access or use, based on a periodic assessment of the adviser information systems and adviser information that resides on the systems. These measures must consider:
- The sensitivity level and importance of adviser information to its business operations.
- Whether any adviser information is personal information.
- Where and how adviser information is accessed, stored and transmitted, including the monitoring of adviser information in transmission.
- Adviser information systems access controls and malware protection; and
- The potential effect a cybersecurity incident involving adviser information could have on the adviser and its clients, including the ability for the adviser to continue to provide investment advice.
- One of the best cyber controls is to establish a hardware/software upgrade cycle that takes security into account. Cyber-attacks are constantly evolving but so are cyber defenses. These defenses are only available on newer hardware/software. The Adviser should create an aged inventory of all hardware/software and establish an upgrade policy.

Data Classification

Data classification is one of the most important steps in Cybersecurity and is an integral part of implementing effective cybersecurity policies and procedures. Data classification is one of the most important steps in Cybersecurity, to understand what our most sensitive data is, where it is, and how well it is protected, Adviser will apply data classifications to identify the sensitivity of information based on the extent to which it's unauthorized disclosure or use may adversely impact the firm's business. Sample data classifications may include the use of data integrity categories such as "Confidential", "Restricted", and "Internal Use Only.

VENDOR MANAGEMENT

- Adviser must perform oversight of service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein and through that oversight document that such service providers, pursuant to a written contract between the adviser and any such service provider, are required to

implement and maintain appropriate measures, including the practices described in paragraphs (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5) of this section, that are designed to protect adviser information and adviser information systems.

- Adviser will follow established procedures using the IT Vendor Due Diligence Questionnaire and document each initial and ongoing review.

THREAT AND VULNERABILITY MANAGEMENT

- Adviser must take measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to adviser information systems and the adviser information residing therein.
- Cybersecurity incident response and recovery.
- Require measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:
- Continued operations of the adviser.
- The protection of adviser information systems and the adviser information residing therein.
- External and internal cybersecurity incident information sharing and communications; and
- Reporting of significant cybersecurity incidents under Rule 204-6 (17 CFR 275.204- 6).
- Require written documentation of any cybersecurity incident, including the adviser's response to and recovery from such an incident.
- Adviser should implement cyber policy auditing software that secures and monitors each endpoint device.
- Adviser has a written Incident Response Plan which will be referenced in response to a cyber incident.
- As part of the incident response plan, the Adviser has a remediation specialist on retainer who will be contacted as needed.
- Adviser has retained cyber liability insurance. The claim will be filed promptly in response to a cyber incident.

INCIDENT REPORTING

- For purposes of this policy, "security breach" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the Adviser. Good faith acquisition of personal information by an employee or agent of Adviser for the purposes of Adviser is not a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.
- Adviser must report to the Commission any significant adviser cybersecurity incident or significant fund cybersecurity incident, promptly, but in no event more than 48 hours, after having a reasonable basis to conclude that any such incident has occurred or is occurring by filing Form ADV-C electronically on the Investment Adviser Registration Depository (IARD);
- Adviser must amend any previously filed Form ADV-C promptly, but in no event more than 48 hours after:
- Any information previously reported to the Commission on Form ADV-C pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity becoming materially inaccurate.

- New material information pertaining to a significant adviser cybersecurity incident or a significant fund cybersecurity incident previously reported to the Commission on Form ADV-C being discovered; or
- Any significant adviser cybersecurity incident or significant fund cybersecurity incident being resolved or any internal investigation pertaining to such an incident being closed.

BOOKS AND RECORDS

The adviser must create and retain:

- A copy of the investment adviser's policies and procedures formulated pursuant to 275.206(4)-7(a) and 206(4)-9 that are in effect, or at any time within the past five years were in effect.
- A copy of the investment adviser's written report documenting the investment adviser's annual review of the cybersecurity policies and procedures conducted pursuant to 275.206(4)-9(b) in the last five years.
- Records documenting the occurrence of any cybersecurity incident, as defined in 275.206(4)-9(c), occurring in the last five years, including records related to any response and recovery from such an incident.
- Records documenting any risk assessment conducted pursuant to the cybersecurity policies and procedures required by 275.206(4)-9(a)(1) in the last five years.

PROHIBITED ACTIONS BY SUPERVISED PERSONS

Supervised persons must not:

- Knowingly commit security violations. This includes one or more of the following:
- Accessing records within or outside the computer and communications facilities for which you are not authorized.
- Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs.
- Violating the privacy of individual users by reading e-mail or private communications unless you are specifically authorized to maintain and support the system.
- Knowingly or recklessly spread computer viruses. To reduce this threat, you may not import files from unknown or questionable sources.
- Transfer personally identifiable information through electronic transmission, other than facsimile, to a person outside of the secure system of the business, unless Adviser uses encryption to ensure the security of the transmission.
- It is not a violation of this policy to transmit the last four digits of a social security number or publicly available information that is lawfully made available to the general public.