Cyber Security & Information Security Policy

Access Persons at Creed Evans Financial include any supervised individuals who meet one or more of the following criteria:

- Have access to non-public information concerning any client's purchase or sale of securities;
- Have access to information about the portfolio holdings of any reportable fund;
- Are involved in making securities recommendations to clients; or
- Have access to non-public securities recommendations.

These individuals are considered Access Persons under the firm's Code of Ethics and are subject to heightened personal trading and reporting obligations to prevent potential conflicts of interest.

Inventory of Technology Infrastructure

On an annual basis, the CCO of Creed Evans Financial will conduct a comprehensive inventory of the following:

- Physical devices and systems, including computers, servers, and other hardware;
- Software platforms and applications used by the firm, such as email, document storage, and file management systems;
- Systems and tools that store or process client data, including client portals and CRM platforms; and
- Third-party vendors and contractors who have access to the firm's technology systems or client data.

This inventory ensures that all technology and access points are properly tracked, secured, and evaluated for compliance with the firm's cybersecurity and privacy protocols.

Creed Evans Financial's primary software platforms that may contain client data are summarized below.

Type of System	Name of System
Customer Relationship Management (CRM)	Google Drive
Custodian interface (Schwab)	Schwab Advisor Network
Email Provider / Hosting	Gmail

Financial Planning	unnamed
Website / Social Media Archiving	unnamed
Document Management / Storage	Google Drive
Portfolio Risk Management	unnamed

Creed Evans Financial utilizes cloud-based technology systems, which offer enhanced information security features, including:

- The ability to leverage the robust infrastructure and expertise of trusted technology industry leaders;
- Advanced system alert capabilities, such as comprehensive user activity logging and real-time alerts for unusual or suspicious activity.

Creed Evans Financial also acknowledges that reliance on cloud-based technology increases the importance of strong password and user authentication controls. In particular, users with administrative access to the firm's cloud systems carry an elevated risk due to their broader access to sensitive client information. Accordingly, the firm has developed, and will continue to enhance, its information security policies to address these heightened risks and safeguard client data.

Information Security Policies

Creed Evans Financial has established the following firm-wide information security policies to safeguard sensitive client data and prevent unauthorized access:

- Staff devices will run up-to-date operating systems with all security patches and software updates set to install automatically.
- Data encryption will be employed on all staff workstations whenever feasible to protect sensitive information.
- Mobile devices used to access work email and files must be password-protected and equipped with remote wipe capability in case of loss or theft.
- Access to Creed Evans Financial systems should be done from private, secure, or known networks. Any access through public networks should be limited and noted for security.
- Staff are required to immediately report any suspicious activity or potential security incidents to the CCO.

Additional Security for Remote Access to Advisory Systems

As a predominantly online service, Creed Evans Financial's business model relies heavily on remote and mobile access to advisory systems. This includes the use of cloud-based file storage, digital identity verification tools, virtual communication platforms, and other technology-driven solutions to facilitate advisor-client interaction and operational efficiency.

Given this model, the firm recognizes the importance of implementing strong security protocols. Accordingly, Creed Evans Financial will:

- Identify any critical systems that must not be accessed remotely
- Power down or disconnect all non-essential hardware when not in use
- Secure all physical storage media and restrict access to office facilities when not in active use
- Ensure all advertising and client communications adhere to firm policies and regulatory requirements
- Maintain complete and secure electronic records of all communications
- Document all client interactions, regardless of the method of communication
- Review and update the Business Continuity Plan as necessary to address evolving risks and operational needs
- Reinforce adherence to cybersecurity best practices, ensuring policies are current and communicated;
- Provide training on information security risks associated with remote work and emphasize protection of non-public client information.
- Use secure internet connections such as trusted WiFi or virtual private networks (VPNs);
- Avoid public WiFi networks due to their vulnerability;
- Store sensitive information on non-company devices only with proper security measures and authorization.

Detection of Unauthorized Activity or Security Breaches

The CCO is responsible for monitoring both on-site and cloud-based systems for suspicious activity and potential security breaches. Examples of unauthorized activity or breaches may include, but are not limited to:

- Logins to company systems outside of traditional business hours for the local region.
- Logins originating from non-local or unexpected geographic regions.
- Large or unusual transfers of files or data.

Upon detection of suspicious activity or a potential breach, the CCO will promptly restrict access to affected systems and initiate an assessment to determine what information may have been compromised and what remediation actions are necessary.

All incidents, regardless of severity, will be thoroughly documented, including:

- The date and time the incident occurred.
- The method by which the incident was detected.
- The nature and severity of the incident.
- The response measures undertaken.
- Any revisions made to the Cybersecurity & Information Security Policy resulting from the incident.

All staff are required to immediately report any suspicious behavior or concerns to the CCO.

If the CCO determines that an incident has resulted in unauthorized disclosure or use of sensitive client information, the following steps will be taken:

- Notify the firm's relevant principals about the incident details.
- Evaluate whether staff disciplinary action is warranted.
- Assess involvement of any third-party vendors in the incident.
- Notify appropriate law enforcement and regulatory agencies as required by law.
- Inform affected clients about the incident and the measures being taken to address it, if necessary.

User Login Security

Creed Evans Financial has implemented the following firm-wide policies to prevent unauthorized access to its systems:

- **Password Requirements:**
    - Must contain both uppercase and lowercase letters
    - Must include at least one number
    - Must include at least one special character
    - Must be at least 8 characters in length
    - Must not include any personal information such as pet names, birthdates, or phone numbers
    - Passwords must be updated at least quarterly
    - Passwords must never be written down
    - Passwords must never be shared with other staff members or third parties

- **Authentication:**
    - Two-factor authentication (2FA) is required wherever available

- **Social Media and Personal Information:**
  Staff must avoid disclosing personal information on social media that could be used to compromise system security. Examples of such information include, but are not limited to:
    - Birthdate
    - Place of birth
    - Wedding location

- Names of schools attended
- Names of close friends or pets
- Favorite drink, song, color, or teacher
- Mother's maiden name
- Make and model of first car

User Access Privileges

Creed Evans Financial has implemented the following user access control policies:

- The CCO is responsible for creating login credentials for all new employees.
- Staff members will be granted access only to the systems necessary to perform their job functions, as determined by the CCO.
- Administrative access privileges will be restricted to the CCO or other authorized personnel designated by the firm.
- Upon termination or departure of any staff member, the CCO will promptly revoke all system access to ensure security.
- Any requests for additional system access must be submitted directly to the CCO for review and approval.

Email Use Security and Guidelines

Creed Evans Financial has implemented the following email use policies:

- Sensitive information must only be transmitted via secure email channels or through a client portal.
- Staff members should never open or download attachments from unknown or suspicious senders.
- Hyperlinks in emails should not be clicked directly without verifying their legitimacy.
- Staff must remain vigilant for phishing attempts designed to capture login credentials.
- Common red flags of phishing emails include:
  - Poor grammar or spelling in the subject line or body
  - Unfamiliar company or website names
  - Suspicious or unusual sender email domains
- Any suspicious emails should be reported to the CCO immediately.

Third-Party Vendor Security and Diligence

Creed Evans Financial enforces the following vendor policies:

- Comprehensive due diligence will be conducted before onboarding any technology vendor and will be reviewed annually thereafter. This due diligence includes evaluation of:
    - The vendor's information security policies
    - Disaster recovery plans
    - Overall capability to meet the firm's operational and security requirements
- All due diligence documentation will be maintained in Creed Evans Financial's vendor diligence file.

Significant Technology System Disruption Plan

In the event of a significant technology disruption, Creed Evans Financial will activate the Business Continuity Plan. If client information is stolen, lost, exposed, or otherwise misused, the CCO will promptly investigate and document the incident. Should a technology system breach occur, the firm will comply fully with all applicable local, state, and federal laws regarding notification of affected parties.