Cybersecurity & Information Security Policy

for Creed Evans Financial Advisory, LLC

Last Updated: February 2, 2026

This Cybersecurity & Information Security Policy describes the administrative, technical, and physical safeguards implemented by the Adviser to protect client nonpublic personal information ("NPI"). The policy is scaled to the firm's size, structure, and risk profile as a single-advisor, state-registered investment advisor.

---

1. Access Persons

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

Access Persons are subject to the firm's Code of Ethics and heightened obligations designed to prevent conflicts of interest and protect client information.

---

2. Inventory of Technology Infrastructure

On at least an annual basis, the Adviser conducts an inventory of technology infrastructure, including:

- Physical devices and systems (computers, mobile devices, hardware)
- Software platforms and applications used by the firm
- Systems that store, transmit, or process client information
- Third-party vendors with access to firm systems or client data

This inventory ensures that all technology and access points are identified, secured, and evaluated for compliance with the firm's cybersecurity and privacy protocols. The firm relies on security controls provided by regulated custodians and widely used technology providers as part of its overall information security framework.

Primary Systems Used by the Firm

Type of System	Name of System
Client communication (email, phone, calendar)	Google Workspace
Document management / storage	Google Workspace
Custody, trading, client account data	Charles Schwab
Electronic execution of client documents	DocuSign
Website hosting	Hostinger

---

3. Cloud-Based Technology Considerations

The firm utilizes cloud-based technology systems that provide enhanced security features, including:

- Robust infrastructure maintained by established technology providers
- Automated alerts and monitoring for unusual or suspicious activity

The firm recognizes that reliance on cloud systems increases the importance of strong authentication and access controls, particularly for administrative accounts. Information security policies are designed to address these risks and safeguard client data.

---

4. Information Security Controls

The firm maintains the following information security practices:

- Devices use current operating systems with security updates enabled
- Encryption is used where supported to protect sensitive data
- Mobile devices accessing firm systems are password-protected and capable of remote wipe
- Access is limited to private, secure, or known networks
- Suspicious activity or security concerns are promptly reported

---

5. Remote Access Controls

The Adviser operates as a fully remote advisory practice and relies on secure remote access to firm systems and client information. Remote access is permitted only through approved devices and systems and is subject to safeguards designed to protect client NPI.

- Access occurs only from private, secure locations
- Public or shared computers are not used
- Devices are protected by passwords, automatic locking, and encryption where supported
- Secure network connections are used
- Public Wi-Fi is avoided or used only with appropriate safeguards
- Multi-factor authentication (MFA) is enabled where supported
- Client information is accessed and stored only through approved, secure platforms.

Remote access controls are reviewed at least annually as part of the Annual Cybersecurity Review. Any suspected loss, theft, unauthorized access, or other cybersecurity incident related to remote access is documented and addressed in accordance with the firm's Incident Response and Cybersecurity policies.

---

6. Detection of Unauthorized Activity & Incident Response

As a single-advisor firm, the Adviser serves as the incident response function and is responsible for identifying, responding to, documenting, and remediating any actual or suspected cybersecurity incidents.

Examples of suspicious or unauthorized activity may include:

- Unexpected login alerts
- Phishing emails requiring action
- Account lockouts from failed logins
- Lost or stolen devices
- Vendor security notifications
- Misrouted emails containing client information
- Unusual file transfers

All incidents are documented, including:

- Date and time
- Method of detection
- Nature and severity
- Response actions taken

- Policy updates, if applicable

Routine system activity (e.g., password updates, routine spam, normal MFA prompts, website traffic logs, standard security summaries) is **not logged** unless associated with a security concern.

If client information is compromised, the Adviser will evaluate notification obligations and comply with applicable laws.

---

7. Authentication & Login Security

Password Standards

Passwords must:

- Include uppercase and lowercase letters
- Include numbers and special characters
- Be at least 8 characters
- Exclude personal information
- Be changed periodically
- Never be shared or written down

Multi-Factor Authentication

Multi-factor authentication is required wherever supported.

---

8. Social Media & Personal Information

Personal information that could compromise security should not be disclosed publicly, including:

- Birthdates or locations
- Names of schools, pets, or relatives
- Personal preferences commonly used for security questions

---

9. User Access Privileges

- Access is granted only as necessary
- Administrative privileges are restricted
- Access is promptly revoked upon termination
- Additional access requires approval

---

10. Email Security Practices

- Sensitive information is transmitted securely
- Attachments and links are verified
- Phishing attempts are reported promptly
- Attachments from unknown or suspicious senders should not be opened or downloaded

---

11. Third-Party Vendor Security

Vendor due diligence appropriate to the firm's size, risk profile and use of the vendor is conducted prior to onboarding and reviewed annually in accordance with the firm's Vendor Management Policy. This due diligence may include 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.

---

12. Business Continuity & Technology Disruption

Significant technology disruptions are addressed under 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.

---

13. Data Backup & Recovery

Firm and client data is backed up in accordance with documented data backup and recovery procedures and reviewed as part of the technology inventory process. Creed Evans Financial stores sensitive firm and client data on both local and third-party systems as documented in the firm's Inventory of Technology Infrastructure.

---

14. Policy Review

This policy is reviewed at least annually as part of the firm's Annual Cybersecurity Review and updated as necessary.