ASPEN CREEK
WEALTH MANAGEMENT

Aspen Creek Wealth Management, LLC

Cybersecurity Policy 2024

950 E. State Highway 114

Southlake, TX, 76092

Phone: 817-400-9905

Email:

william.tyler@aspencreekwealth.com

www.aspencreekwealth.com

Table of Contents

Firm Cybersecurity Policies

Aspen Creek Wealth Management's ("ACWM") policy is to respond to the increase in cybersecurity breaches. We have developed this policy first and foremost to ensure the security of our clients' information that is maintained electronically.

Acceptable Use Policy

The Chief Compliance Officer's ("CCO") intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to ACWM's established culture of openness, trust and integrity. The CCO is committed to protecting ACWM's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of ACWM. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every ACWM employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of computer equipment at ACWM. These rules are in place to protect the employee and ACWM. Inappropriate use exposes ACWM to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy applies to the use of information, electronic and computing devices, and network resources to conduct ACWM business or interact with internal networks and business systems, whether owned or leased by ACWM, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at ACWM and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with ACWM policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at ACWM, including all personnel affiliated with third parties. This policy

applies to all equipment that is owned or leased by ACWM as set forth in the attached Technology Inventories.

General Use and Ownership

ACWM proprietary information stored on electronic and computing devices whether owned or leased by ACWM, the employee or a third party, remains the sole property of ACWM.

You have a responsibility to promptly report the theft, loss or unauthorized disclosure of ACWM proprietary information.

You may access, use or share ACWM proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

For security and network maintenance purposes, authorized individuals within ACWM may monitor equipment, systems and network traffic at any time.

ACWM reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Propriety Information

System-level and user level passwords must comply with the Password Construction Guidelines and Password Protection Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

Postings by employees from a ACWM email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of ACWM, unless posting is in the course of business duties.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of ACWM authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing ACWM-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ACWM.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ACWM or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting ACWM business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.

7. Using a ACWM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any ACWM account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to the CCO or delegate is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the ACWM network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, ACWM employees to parties outside ACWM.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation with the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within ACWM's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by ACWM or connected via ACWM's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Social Media and Blogging

1. Social media use and blogging by employees, whether using ACWM's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of ACWM's systems to engage in social media use and blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate ACWM's policy, is not detrimental to ACWM's best interests, and does not interfere with an employee's regular work duties. Social media use and blogging from ACWM's systems is also subject to monitoring.

2. ACWM's Confidential Information policy also applies to social media use and blogging. As such, Employees are prohibited from revealing any ACWM confidential or proprietary information, trade secrets or any other material covered by ACWM's Confidential Information policy when engaged in social media use and/or blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of ACWM and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or engaging in social media use.

4. Employees may also not attribute personal statements, opinions or beliefs to ACWM when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of ACWM. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, ACWM's trademarks, logos and any other ACWM intellectual property may also not be used in connection with any social media activity

Responsibility

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Clean Desk Policy

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

This policy applies to all ACWM employees and affiliates.

1. Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
2. Computer workstations must be locked when workspace is unoccupied.
3. Computer workstations must be shut completely down at the end of the workday.
4. Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
5. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
6. Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
7. Laptops must be either locked with a locking cable or locked away in a drawer.

8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
9. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
10. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
11. Whiteboards containing Restricted and/or Sensitive information should be erased.
12. Lock away portable computing devices such as laptops and tablets.
13. Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

Responsibilities

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Wireless Communication Policy

The purpose of this policy is to secure and protect the information assets owned by ACWM provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. ACWM grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the CCO are approved for connectivity to a network.

All employees, contractors, consultants, and temporary workers at ACWM, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the firm must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a network or reside on a site that provides wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

General Requirements

All wireless infrastructure devices that reside at a site and connect to a network, or provide access to information classified as Confidential, or above must:

1. Abide by the standards specified in the Wireless Communication Standard.
2. Use approved authentication protocols and infrastructure.
3. Use approved encryption protocols.
4. Maintain a hardware address (MAC address) that can be registered and tracked.
5. Not interfere with wireless access deployments maintained by other support organizations.

Wireless Communication Standard

All wireless infrastructure devices that connect to a network or provide access to Confidential Information must:

1. Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAPFAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
2. Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
3. All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to the corporate network, must:

1. Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAPTLS
2. When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
3. Disable broadcast of SSID
4. Change the default SSID name
5. Change the default login and password

Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the corporate network. Access to the corporate network through this device must use standard remote access authentication.

Responsibilities

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Remote Access Policy

Remote access to our corporate network is essential to maintain productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of ACWM's policy, we must mitigate these external risks to the best of our ability.

The purpose of this policy is to define rules and requirements for connecting to ACWM's network from any host. These rules and requirements are designed to minimize the potential exposure to from damages which may result from unauthorized use of resources. Damages include the loss of sensitive or confidential information, intellectual property, damage to public image, damage to critical internal systems, and fines or other financial liabilities incurred as a result of those losses.

This policy applies to all employees, contractors, vendors and representatives with a ACWM-owned or personally-owned computer or workstation used to connect to the network. This policy applies to remote access connections used to do work on behalf of ACWM, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to networks.

It is the responsibility of employees, contractors, vendors and representatives with remote access privileges to ACWM's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to ACWM. General access to the Internet for recreational use through the network is strictly limited to employees, contractors, vendors, representatives, and clients (hereafter referred to as "Authorized Users"). When accessing the network from a personal computer, Authorized Users are responsible for preventing access to any computer resources or data by non-Authorized Users. Performance of illegal activities through the network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy.

Requirements

1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Encryption Policy and the Password Policy.

2. Authorized Users shall protect their login and password, even from family members.
3. While using a ACWM-owned computer to remotely connect to ACWM's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
4. Use of external resources to conduct business must be approved in advance by CCO and the appropriate business unit manager.
5. All hosts that are connected to internal networks via remote access technologies must use the most up-to-date anti-virus software as indicated by the CCO and all systems and software must be fully patched, this includes personal computers.

Responsibilities

The CCO or delegate will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Third-Party Vendor Policy

This policy applies to contractors, consultants, temporaries, and other third-party vendors (collectively referred to as "vendors") providing services for ACWM. Vendors must comply with all applicable ACWM cybersecurity policies, practice standards and agreements, including, but not limited to:

- Acceptable Use Policies
- Network access policies such as our Wireless Communication and Remote Access Policies

All vendors used by ACWM will be cataloged in the attached Third-Party Vendor Inventory.

Third-Party Agreements and Contracts

Vendor agreements and contracts must specify:

- ACWM-owned information that the vendor is permitted to access

- How ACWM's information is to be protected by the vendor
- The vendor's security incident and response plan with regard to ACWM's information
- Acceptable methods for the return, destruction or disposal of ACWM's information in the vendor's possession at contract termination
- Confirmation that the vendor must only use ACWM's information for the intended purpose and duration of the agreement
- Confirmation that any additional ACWM information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
- If a vendor is involved in ACWM's security incident management, the responsibilities, deliverables details, regular work hours, and duties must be specified.

ACWM will provide a point of contact for the vendor. The point of contact will work with the vendor to confirm the vendor is in compliance with these policies.

Vendor Employees

Vendors must provide ACWM with a list of all employees assigned to the contract. The list must be updated and provided to the CCO within 24 hours of staff changes. On-site vendor employees must acquire an identification badge that will be displayed at all times while on the premises. The badge must be returned when the employee leaves the contract or at the end of the contract.

Each vendor employee with access to ACWM confidential information must be cleared to handle that information by the CCO.

Vendor employees must report all security incidents affecting ACWM directly to the CCO.

Vendor Access – Security Incident Management

The following standards pertain to vendors contracted to assist ACWM in the case of a security incident.

All vendor equipment and/or software on ACWM's network that connects to the outside world via the network, telephone line, or leased line, and ACWM's vendor accounts will remain disabled except when in use for authorized use.

Vendor access must be uniquely identifiable and must comply with the ACWM Password Construction Guidelines and Password Protection Policy. Vendor's major work activities must be entered into a log and available to ACWM upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.

Vendor Termination

Upon the departure of a vendor employee from the contract for any reason, the vendor will provide a written certification that all ACWM information is collected and returned to ACWM or destroyed within 24 hours of the employee's departure.

Upon termination of contract, or at the request of ACWM, the vendor will return or destroy all ACWM information and provide a written certification of that return or destruction within 24 hours.

Upon termination of contract, or at the request of ACWM, the vendor must surrender all ACWM identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by the CCO.

All software used by the vendor in providing service to ACWM must be properly inventoried and licensed.

Responsibilities

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

Any vendor found to have violated this policy may be subject to actions, up to and including termination of contract.

Digital Signature Policy

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in ACWM electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

This policy applies to all ACWM employees and affiliates.

A digital signature is an acceptable substitute for a wet signature on any firm document or correspondence.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CCO) are not considered valid.

Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

Signer Responsibilities

1. Signers must obtain a signing key pair from ACWM. This key pair will be generated using ACWM's Public Key Infrastructure (PKI) and the public key will be signed by the ACWM's Certificate Authority (CA), <CA Name>.
2. Signers must sign documents and correspondence using software approved by ACWM.
3. Signers must protect their private key and keep it secret.
4. If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact ACWM's CCO immediately to have the signer's digital key pair revoked.

Recipient Responsibilities

1. Recipients must read documents and correspondence using software approved by ACWM.
2. Recipients must verify that the signer's public key was signed by the ACWM's Certificate Authority (CA) by viewing the details about the signed key using the software they are using to read the document or correspondence.
3. If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.
4. If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to ACWM's CCO.

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO ore delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Password Construction Guidelines

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems or data. The purpose of this guideline is to provide best practices for creating strong, secure passwords.

This guideline applies to employees, contractors, consultants, and temporary workers. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

Statement of Guidelines
All passwords should meet or exceed the following guidelines:

Strong passwords have the following characteristics:

- Contain at least 12 alphanumeric characters.
- Contain both upper and lower case letters.
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Poor, or weak, passwords have the following characteristics:

- Contain less than eight characters.
- Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Are some version of “Welcome123” “Password123” “Changeme123”

You should never write down a password. Instead, try to create passwords that you can remember easily. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

(NOTE: Do not use either of these examples as passwords!)

Passphrases

Passphrases generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access.

A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheRoad2SuccessIs@lwaysUnderConstruction!).

Responsibilities

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Password Protection Policy

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of ACWM's resources. All users, including contractors and vendors with access to ACWM systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ACWM facility, has access to the ACWM network, or stores any non-public ACWM information.

Password Creation

All user-level and system-level passwords must conform to the Password Construction Guidelines.

1. Users must not use the same password for ACWM accounts as for other non-ACWM access (for example, personal ISP account, option trading, benefits, and so on).
2. Where possible, users must not use the same password for various ACWM access needs.
3. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to access system-level privileges.

Password Change

1. All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
2. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
3. Password cracking or guessing may be performed on a periodic or random basis by the CCO or delegate or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

Password Protection

1. Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential ACWM information. ACWM recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.
2. Passwords must not be inserted into email messages or other forms of electronic communication.
3. Passwords must not be revealed over the phone to anyone.
4. Do not reveal a password on questionnaires or security forms.
5. Do not hint at the format of a password (for example, "my family name").
6. Do not share ACWM passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
7. Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
8. It is acceptable to use certain encrypted password managers available on the internet. The CCO or delegate will provide a list of acceptable providers upon request.

9. Do not use the "Remember Password" feature of applications (for example, web browsers).
10. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

All of the rules above that apply to passwords apply to passphrases.

Responsibilities
The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Confidentiality Policy

The firm maintains safeguards to comply with federal and state standards to guard each client's information. The firm does not share any information with any nonaffiliated third parties, except in the following circumstances:

- As necessary to provide the service that the client has requested or authorized, or to maintain and service the client's account;
- As required by regulatory authorities or law enforcement officials who have jurisdiction over the firm, or as otherwise required by any applicable law; and
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Employees are prohibited, either during or after termination of their employment, from disclosing client information to any person or entity outside the firm, including family members, except under the circumstances described above. An employee is permitted to disclose information only to such other employees who need to have access to such information to deliver our services to the client.

Responsibilities
The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Acceptable Encryption Policy

The purpose of this policy is to provide guidance that limits the use of encryption to protect information resources that contain, process, or transmit confidential information. Additionally, this policy provides direction to ensure that Federal regulations are followed

This policy applies to all ACWM employees and affiliates. It addresses firm data that is at rest (in portable devices, removable media, etc.), data in motion (i.e. transmission security), and encryption key standards and management.

ACWM uses AES technology for encrypting confidential and other firm sensitive data, unless an exception is provided by the CCO. Symmetric cryptosystem key lengths should be at least 80 bits for confidential data and 64 bits for other sensitive information identified by the firm. Asymmetric crypto-system keys must be of a length that yields equivalent strength, (e.g., approximate equivalencies of 64 bit symmetric = 512 bit asymmetric; 80 bit =1024 bit; 112 bit = 2048 bit; 128 bit = 3072 bit).

All encryption mechanisms implemented to comply with this policy support a minimum of, but not limited to the industry standard, AES 128-bit encryption.

Data at Rest

In an attempt to prevent information spillage from the encrypted region into the unencrypted region ACWM requires full disk encryption.

Confidential data at rest on computer systems owned by and located within ACWM controlled spaces and networks must be protected by encryption with strict access controls that authenticate the identity of those individuals accessing the data. This is in addition to passwords/passphrases in-line with our policies

ACWM secures its back up and/or stored data on disks and/or drives in a cloud environment. Confidential Information back-up data is protected using AES 256-bit algorithm or identical live data encryption methodologies.

Computer hard drives or other storage media that have been encrypted shall be sanitized to prevent unauthorized exposure in accordance with our safe disposal guidelines.

Portable Devices

The best way to prevent unauthorized exposure to Confidential Information located on portable devices is to avoid storing Confidential Information on these devices. As a general practice, Confidential Information should not to be copied to or stored on a portable computing device or a non-ACWM owned computing device. However, in situations that require Confidential Information to be stored on such devices,

encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

All users must obtain specific permission from the CCO before storing Confidential Information on a portable computing device or a non-ACWM owned computing device.

Confidential Information stored on portable devices including laptops, tablets and smartphones must be encrypted using products and/or methods approved by the CCO including full disk encryption with pre-boot authentication.

Portable devices including, laptops, tablets, and smartphones should not be used for the long-term storage of any Confidential Information.

Should these devices store or transmit Confidential Information, they must have the proper protection mechanisms installed, including password protection, antivirus or firewall software, and dual authentication controls subject to needed applications being properly configured.

Removable media including CD-ROMs, DVDs, and USB memory drives that contain Confidential Information must be encrypted and stored in a secure, locked location.

ACWM will inventory encrypted devices and validate the implementation of encryption products at least annually.

Data Transmission

Users will follow ACWM's Acceptable Use Policies when transmitting data and must take particular care when transmitting or re-transmitting Confidential Information received from non-firm employees and Clients.

Confidential Information transmitted as an email message must be encrypted.

Any Confidential Information transmitted through a public network (e.g., Internet) to and from vendors, Clients, or entities doing business with ACWM must be encrypted or be transmitted through an encrypted tunnel that is encrypted with either of the following methods of encryption: virtual private networks (VPN) or point-to-point tunnel protocols (PPTP) like secure socket layers (SSL).

Transmitting unencrypted Confidential Information through the use of web email programs, (Yahoo, Gmail, etc.) is not allowed.

Encryption Key Management

Effective key management is the crucial element for ensuring the security of any encryption system. These key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements. ACWM key management systems are characterized by the following security precautions:

1. The CCO will verify backup storage for key passwords, files, and related backup configuration data to avoid single point of failure and ensure access to encrypted data.
2. No single individual, other than the CCO, is authorized to generate a new CA key pair.
3. Regular annual audit trail reviews are conducted.
4. Key management should be fully automated, e.g., ACWM personnel do not have the opportunity to expose a key or influence the key creation.
5. Keys in storage and transit must be encrypted.
6. Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.
7. Private keys must be kept confidential

Responsibilities

The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Data Backup Policy

The purpose of this policy is to establish the requirement that all of ACWM's data is regularly backed-up and recoverable in the case of a data breach or disaster.

This policy applies to all ACWM systems and data.

1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
2. There must be multiple backups of critical information, preferably with different media, vendors and designated personnel within each node responsible for backing up data. The persons responsible for backing up data should be independent and not have access to the other's backups.
3. The ACWM backup and recovery process for each system must be documented and periodically reviewed.
4. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems.
5. A process must be implemented to verify the success of the ACWM electronic information backup.
6. Backups must be periodically tested to ensure that they are recoverable.

7. Employees approved for access to ACWM backup media held by the offsite backup storage vendor(s) must be reviewed annually or when an authorized individual is terminated or leaves employment.

Responsibilities
The CCO or delegate will verify compliance with this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Data Assessment and Breach Response Policy

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

ACWM's intentions for publishing a Data Assessment and Breach Response Policy are to focus significant attention on data security and data security breaches and how ACWM's established culture of openness, trust and integrity should respond to such activity. ACWM is committed to protecting ACWM's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that theft, breach or exposure of ACWM confidential information has occurred must immediately provide a description of what occurred via e-mail to the CCO who will investigate to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the CCO will follow the appropriate procedure in place.

This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle confidential information of ACWM clients. Any agreements with vendors will contain language similar that protects the fund.

As soon as theft, data breach or exposure containing ACWM confidential information is identified, the process of removing all access to that resource will begin.

Periodic Assessments

At least annually, ACWM will conduct assessments to detect potential systems vulnerabilities and to ensure that cybersecurity procedures and systems are effective in protecting confidential information. These assessments ACWM will then respond to deficiencies detected through such assessments by taking timely corrective action in response to detected deficiencies.

Breach Response

ACWM's response to data breaches will depend upon the type and severity of the incident. The CCO will be notified of the theft, breach or exposure and will analyze the breach or exposure to determine the root cause, how the incident occurred, the types of data involved, the number of internal/external individuals and/or organizations impacted, and analyze the breach or exposure to determine the root cause. In responding, ACWM will:

- Contain and mitigate the incident/breach to prevent further damage
- Evaluate incident and understand potential impact
- Implement a disaster recovery plan (if needed)
- Alert the proper authorities (regulator, local law enforcement, FBI, United States Secret Service)
- Determine if the personal information of customers was compromised and notify affected customers within 30 days of the date the firm became aware of the breach
- Enhance systems and procedures to help prevent the recurrence of similar breaches
- Evaluate response effort to and update response plan to address any shortcomings

Responsibilities

The CCO or delegate will verify compliance with this policy through risk assessments, monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Any exception to the policy must be approved by the CCO or delegate in advance.

Any ACWM personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

Approval

By: _____
Name: William Tyler
Title: Chief Compliance Officer