AXXCESS
WEALTH MANAGEMENT

Axxcess (AWM) Cybersecurity Policy Overview and Update- 2020

Questions for you to consider as you review the updates outlined below.

1) Data - This is the sensitive information we hold for clients like SSNs, DOBS, account numbers, transactions, money movements, client notes, contact lists and more.

Relevant questions: Where is my data in space and time? On what specific drives? Utilizing what database technologies? Accessible remotely by what tools and people?

2) Application Security - These are the controls within your line-of-business applications like practice management, time and billing, accounting, document management, e-discovery, and so on.

Relevant questions: Have we setup security profiles, access rights, permissions, ethical walls and passwords? Do we have or need dual-factor authentication? How are we sharing important documents and emails with clients?

3) IT Infrastructure Security - These are the actual hardware and software assets you employ for security like antivirus, antispam, firewall, content filtering, patch & vulnerability management, encryption, physical security and more.

Relevant questions: Am I proactively managing security? Is the firewall fully employed or is it just on? Are we testing for new vulnerabilities on an ongoing basis? Do we have encryption for data at rest?

4) Education & Policy Enforcement - Refers to what we are here for today; the creation of firm policies and plans that constitute the firm's Cybersecurity Framework, such as written security policies, incident response plan, disaster recovery plan and more.

Relevant questions: Are firm members trained on proper security? Do they know how to identify a malicious email or how to respond if they believe a virus has infected their PC? Are our policies adequate, written, updated and enforced?

5) Continual Assessment & Improvement - Finally, firms need an ongoing process for the testing of new attack vectors, the effectiveness of the CS Framework, and testing for weaknesses in the approach.

Relevant questions: Have new threats emerged? Do recent close-calls warrant a review of our practices? In spite of our efforts and security spend, are our Advisors and staff really knowledgeable and therefore safe? Have any of the new programs or services we purchased this year compromised our security posture? The purpose of this handbook is to assist both Advisors and staff with a set of procedures to stay vigilant and aware of an ongoing, and evolving area of risk.

CYBER SECURITY GUIDELINES AND REQUIREMENTS

Updated 10/2020

I. INTRODUCTION

The following guidelines and requirements ("CSG&R") set out to protect the security and integrity of confidential information of Axxcess Wealth Management, LLC ("the Firm"), as well as that of our clients. With increased use of technology by registered investment companies, funds and advisers need to protect confidential and sensitive information related to their activities from third parties, including information concerning fund investors and advisory clients.

II. CYBER SECURITY GUIDANCE

1. There are a number of measures that the firm may conduct periodically to address cyber security risks, including, but not limited to:
   - The nature, sensitivity and location of information that the firm collects, processes, stores, and the technology systems in use
   - Internal and external cyber security threats to the firm's information and technology systems
   - Security controls and processes currently in place
   - The impact of a system being compromised

An effective assessment of risk would assist in identifying potential cyber security threats and vulnerabilities so as to mitigate risk in a maximum capacity,

- Axxcess has created a strategy designed to help prevent, detect, and respond to cyber security threats. Our objectives include:
- Controlling access to various systems and data via management of user credentials, authentication, and authorization methods, firewalls, tiered access to sensitive information and network resources, and network segregation.
- Data encryption.
- Addressing mobile access risks
- Protecting against the loss of sensitive data by restricting use of removable storage media.
- Data backup and retrieval; and
- The development of an incident response plan.

Implement AWM's strategies through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats. Advisers may wish to educate their investors and clients about how to reduce their exposure to cyber security threats concerning their accounts.

III. COMPLIANCE WITH AWM'S CYBER SECURITY GUIDELINES & REQUIREMENTS

- AWM has updated its requirements for Advisors, Employees, and any person accessing client data electronically must have every device password protected and must prevent unauthorized access to any device that is used to access client data by family members, guests, and other employees.
- All persons accessing the internet must do so behind a modem/router that is password protected and encrypted.
- All persons accessing the internet must do so behind a device that is password protected using multi factor, contextual, or biological encryption.
- All persons must use Multi Factor Authentication when accessing client data from any systems which include custodial, CRM, trading, and email systems.

The following outlines a summary of our updated policies which apply to all persons accessing client data. The actual policy language follows after the summaries:

A. Email Policy: Email is the primary means of communication at the firm. Guidance is necessary for compliance reasons as well as congruity. This covers passwords for emails, acceptable use for emails, content restrictions, backup and monitoring. Consider including policy statements as it relates to email that discuss acceptable content to be shared over email, email encryption, phishing and attachment handling.

a. *Real world use: A firm wants to find all emails related to a case; they can perform a conflict check and export records, but wouldn't it be helpful if employees already had this information readily available? An email policy for retention can standardize the ways you save making finding what you need that much easier.*

B. Anti-Malware/Anti -Virus Policy: Malware is software written with malicious intent. Computer viruses, Trojan horses, worms, and spyware are examples of malware. The policy states the requirements for controls to prevent and detect the dissemination of any malicious software on firm computer and communications systems found on firm assets. The anti-malware policy governs the centralized anti-malware system in place at the firm and should include guidelines for updates, rules for quarantining and/or removal, and communication efforts if malware is detected.

a. *Real world use: Malware can be installed by clicking a link in a phishing email, or by clicking an ad that looks legitimate, or by other means. In order to effectively combat this attack vector, you will need to establish rules for using IT at the firm.*

C. Clean Desk & Clear Screen Policy Clean desks are the cornerstone of a secure workplace. In efforts to minimize the unauthorized sharing of classified information, clean desks are required. Guidelines are needed to accomplish clean desks and clear screens. Statements regarding screen locking and the use of post-it notes that contain sensitive information are a part of this policy.

D. Cloud Services: This policy applies to all external cloud services (e.g. cloud-based email, document storage, etc.). Personal accounts are excluded. This policy provides guidance for how to handle any services related to remote servers storing sensitive firm data. The cloud services policy should layout the firm's position of non-managed cloud services, such as Gmail or DropBox. Expectations that work-related materials should not be transmitted over non-managed cloud services is a critical part of the policy.

a. *Real world use: Many firms have consumer tools like Dropbox, Box, Drive and other cloud apps. Staff and partners alike may be unknowingly exposing your sensitive data. Having a policy forces everyone to uses industry best practices.*

E. Encryption Policy: This policy defines the requirements for establishing the encryption implementation and management requirements related to the firm computer and communications systems infrastructure. By setting standards, the firm maintains the most relevant encryption technology is used. Define places within the firm infrastructure where encryption is warranted, such as laptops, email, HR data, and other places where critical or otherwise sensitive data is stored. Real world use: A firm has emphasized data encryption as an asset in its war against cyber criminals. But Sheila has no password on her phone where some of that data resides. Hackers log into her phone and bypass encryption. A policy ensures you can adequately defend against this attack vector.

F. Mobile Device Policy Mobile devices are assets that the firm utilizes on an everyday basis. This policy determines the information security requirements for the protection of sensitive information while being transmitted or received over any type of mobile device. A mobile device policy should detail how mobile devices are issued and managed. Password and access controls should also be defined. Mobile app installations guidelines and mobile device wiping and reset guidelines should also be included. Any features of Mobile Device Management (MDM) plan should be documented: encryption, password expiry, content filtering, whitelisting, and more. Moreover, each class of data available to the device should be defined and policies around it enforced (i.e., Exchange sync, mobile app, emails, etc.).

   a. Real world use: A firm has mobile devices with client, event, and task data. A phone is stolen and the attorney knows an important merger and acquisition document was present on the device. How can the data be removed?

G. Password Management Policy: Passwords are the primary token used to access firm information systems. How passwords should be handled must be properly coordinated and supported. Outlining specifics on how passwords should be managed by each employee is central to staying secure and compliant. Password policies should describe how user passwords are created and managed. Include definitions on acceptable password characteristics such as password length, complexity, and a password-change schedule.

   a. Real world use: A firm has one password to log on to Windows which enables password-free login to all applications and databases. The password hasn't been changed in three years. Worried yet? Maybe the password is 'password' – how about now?

H. Removable Media Policy This policy defines the requirements for the proper handling of all media that contains firm information. In most organizations, information is generated and stored on many different types of media including paper documents, computer media, and a myriad of portable devices. Much of this information is considered confidential or sensitive, which requires that its handling is performed in a safe and secure manner. The removable media policy should detail how the firm and firm member handle removable media such as USB drives and DVDs or CDs. Consider creating statements that restrict or control the use of USB thumb drives.

   a. *Real world use: A firm has prohibited using flash drives to store information of any kind, but has no media policy in place and therefore has implemented no security controls. This means the firm is relying on the honor system rather than using centralized management to disable the use of any media.*

I. Social Media Policy Social Media is a predominant part of popular culture and becoming an integral part of business. Firms use social media as means to advertise and keep in touch with clients. Firm policy statements on social media should protect the firm from the dissemination of sensitive information and/or damaging the firm's reputation.

   a. Real world use: a firm encourages staff and attorneys to have a social media presence. A staff member happily announces to her 500 followers that the firm is helping merge two pharmaceutical companies. This sends one of the company's stock prices into a spiral and jeopardizes the deal; the company is talking about suing the firm for its market value loss.

J. Wireless Communication Policy Firm members are constantly part of a connected world. This policy addresses the use of mobile communication devices via wireless communication either Wi-Fi internet or Bluetooth for business purposes – and methods for securing the communicated information. This policy should describe how the firm protects its assets from unauthorized access over Wi-Fi and other wireless vectors. Statements should include the firm's position on personal hotspots and use of guest networks.

Policy Introduction

- AWM requires that any device used to access client data have at minimum:
  a. antivirus software on each device used to access confidential and sensitive information of the Firm and/or its clients. The minimum features in the required antivirus software must include the following:
     - Block ransom ware and viruses
     - Protect your identity
     - Protect social networks
     - Provide safe Wi-Fi access
     - Provide Botnet Protection
     - Provide protection of home router and webcam
     - Provide online shopping safety
     - Include anti malware protection

AWM requires that each employee who accesses any proprietary and sensitive Firm or client information on their personal devices, (cell phones, iPads, etc) MUST have that specific device password protected that has an auto lock feature after non use.

Email Policy:

BACKGROUND: Email is the primary method of electronic communication with all types of business. Axxcess is required to archive email correspondence as a part of its regulatory obligations. How users communicate in a professional manner is important, and this policy outlines policies that best reflect you , your advisory busines and Axxcess.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by Axxcess.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER Director

EFFECTIVE DATE (Determined by Director)

REVIEW DATE Annual Review

POLICY STATEMENTS: Axxcess requires that all business related correspondence be conducted on company approved business email and email domains. This includes prospecting, advertising, marketing, and anything communication that could remotely be connected to the business of financial services occur on approved email. Personal email must not be used for any business related communication of any kind. Axxcess recognizes that employees may have personal email accounts on a variety of Web-based email accounts such as Gmail, Outlook.com, Apple Mail, Hotmail and Yahoo. Axxcess understands that employees may want to use those accounts during work utilizing the personal devices or company assets. It is approved to use personal email on company assets only if used for personal use. Personal use of email should be reserved during non business periods.

Email Policy – Any electronic communication with a client or prospect must exclusively be conducted on approved business email. There is a zero tolerance policy for conducting any communication with a client or prospect on personal, non-approved email. If such communication occurs inbound from a client or prospect on personal email, supervised persons must immediately forward that email to the approved business account and ensure that future correspondence occur on the business account. Axxcess users and approved Axxcess DBAs shall have no expectation of privacy in regards to information that they input or review while using approved business email, this includes information on the sender, subject, content, or other information that is entered or transmitted from any device. Disclosures to this effect must be in place at all times on newly sent, and reply emails. The approved disclosures are as follows and customized in the case that a supervised person is affiliated with an broker dealer.

> CONFIDENTIALITY NOTICE: This email may contain privileged or confidential information and is for the sole use of the intended recipient(s). Any unauthorized use or disclosure of this communication is prohibited. If you believe that you have received this email in error, please notify the sender immediately and delete it from your system.
>
> NO OFFER OR SOLICITATION: The contents of this electronic mail message: (i) do not constitute an offer of securities or a solicitation of an offer to buy securities, and (ii) may not be relied upon in making an investment decision related to any investment offering Axxcess Wealth Management, LLC, an SEC Registered Investment Advisor. Axxcess does not warrant the accuracy or completeness of the information contained herein. Opinions are our current opinions and are subject to change without notice. Prices, quotes, rates are subject to change without notice. Generally, investments are NOT FDIC INSURED, NOT BANK GUARANTEED and MAY LOSE VALUE. Brokerage services are offered through BROKER DEALER OF YOUR LIKING, LLC a registered Broker Dealer, member FINRA, SIPC, NFA.
>
> All e-mail sent to and from this address will be received or otherwise recorded by Axxcess Wealth Management , LLC. and is subject to archival, monitoring or review by, and/or disclosure to, someone other than the recipient. This e-mail and attachments are confidential and may be protected by legal privilege. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of this e-mail or any attachment is prohibited. If you have received this e-mail in error, please notify us immediately by returning it to the sender and delete this copy from your system. Thank you for your cooperation. YOUR FAVORITE BROKER DEALER and Axxcess Wealth Management, LLC are not affiliated. Advisory services offered independent of THE BROKER DEALER YOU TOLERATE, LLC

Axxcess Code of Ethics, and Axxcess Policy and Procedure Manual all outline strict rules for monitoring all data in and out of the network; this applies to all email accessed from inside or outside Axxcess systems.

Email Communication – You must conduct yourself professionally at all times, avoiding using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or competitors, or that might constitute harassment or bullying. Axxcess expects all users to act in a morally exemplary manner wherever they may express themselves. Examples of in-appropriate conduct include offensive communication meant to intentionally harm someone's reputation or communication that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

Sensitive Information on email – You must maintain the confidentiality of Client data, account information, and comply at all times with company policy as well as securities laws regarding safe guarding of customer data, advertising and marketing. When transmitting client data which include account numbers, DOB, or SS, you must encrypt your email. Sharefile Encryption for outlook is the only currently approved encryption application approved by Axxcess. Sharefile outlook plugin is accessible at Axxcess.sharefile.com at no additional cost and must be installed on outlook, and is the only approved method to send emails with PII. You must at all times protect private or confidential information. You must protect methods and internal processes and Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications through email, or any other system not approved by Compliance.

Company Opinions - Express only your professional opinions. Never represent yourself as a spokesperson for Axxcess.

Email Advertising – Any email being sent to more than 10 clients or prospects must be submitted for approval prior to sending at hub.axxcessplatform.com. Only approved content may be sent.

EXCEPTIONS: You main submit for approval business related emails which will be subject to review, approval and monitoring.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

A. Anti-Malware/Anti -Virus Policy: Malware is software written with malicious intent. Computer viruses, Trojan horses, worms, and spyware are examples of malware. The policy states the requirements for controls to prevent and detect the dissemination of any malicious software on firm computer and communications systems found on firm assets. The anti-malware policy governs the centralized anti-malware system in place at the firm and should include guidelines for updates, rules for quarantining and/or removal, and communication efforts if malware is detected.

Anti Malware/Anti Virus Policy:

BACKGROUND: Malware is software written with malicious intent. Computer viruses, Trojan horses, worms, and spyware are examples of malware. The policy states the requirements for controls to prevent and detect the dissemination of any malicious software on firm computer and communications systems found on firm assets. The anti-malware policy governs the centralized anti-malware system in place at the firm and should include guidelines for updates, rules for quarantining and/or removal, and communication efforts if malware is detected.

How users behave while online is the first and best defense against cyber intrusions and your vigilance are the best defense against compromise.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: Any online activity represents the potential for compromise. Clicking, visiting, opening an email, attachment, or link can contain malware or virus that can lead to a compromise of data.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Cyber Security Policy, Axxcess Policy and Procedure Manual all outline strict rules for monitoring all data in and out of the network; this applies to all methods and devices used to access client data from inside or outside Axxcess systems.

Axxcess has selected ESET Corporate Endpoint Security as its corporate anti virus and mal ware suite. Axxcess will provide and it is mandatory to install and continuously update corporate end point security on any device that accesses client data. You must not access client data from a public computer, or public device that is not secured by Eset Corporate Endpoint Security. All workstations and laptops accessing client data, online business systems, or applications must have Eset Endpoint Security installed and active. Anti Malware and Anti Virus definitions will automatically update daily. On occasion, potential threats will be identified and quarantined. If local user action (you, your computer or device) is warranted, your prompt action, and attention are required. Your browsing habits and ongoing attention and vigilance during and importantly in off hours internet sessions is necessary to avoid compromise. No software or system is impenetrable. Only your attention to details can help prevent data breaches and compromise. You are required to report any malware or virus attacks or infections on any device that is compromised immediately. That device must be immediately identified.

Any email you receive that is suspicious must be forwarded to compliance@axxcesswealth.com prior to opening any attachments or clicking links.

Axxcess will test and re-test your compliance with best practices. You must continually review and prevent attempts to compromise client data, which include avoiding downloading applications unknown to you, being vigilant and current on phishing schemes and cyber-crimes used to compromise client data. Completion of any assigned training in a timely manner is mandatory.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

Clean Desk Policy:

BACKGROUND: Clean Desk & Clear Screen Policy Clean desks are the cornerstone of a secure workplace. In efforts to minimize the unauthorized sharing of classified information, clean desks are required. Guidelines are needed to accomplish clean desks and clear screens. Statements regarding screen locking and the use of post-it notes that contain sensitive information are a part of this policy.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: 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.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Clean Desk Policy, Axxcess Policy and Procedure Manual all outline strict rules for monitoring all data in and out of the network; this applies to all methods and devices used to access client data from inside or outside Axxcess systems.

- Computer workstations must be locked when workspace is unoccupied.
- 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 work day.
- File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to restricted or sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- 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.
- Printouts containing restricted or sensitive information should be immediately removed from the printer.
- Upon disposal restricted and/or sensitive documents should be shredded in the official shredder bins or placed in the locked confidential disposal bins.
- Whiteboards containing restricted and/or sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CD, DVD or USB drives as sensitive and secure them in a locked drawer and always use external devices with full disk encryption.
- USB or external devices without full disk encryption should be re-formatted, retired, and not used for any business purposes.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

Cloud Services Policy:

BACKGROUND: Cloud Services: This policy applies to all external cloud services (e.g. cloud-based email, document storage, etc.). Personal accounts are excluded. This policy provides guidance for how to handle any services related to remote servers storing sensitive firm data. The cloud services policy lays out the firm’s position of non-managed cloud services, such as Gmail or DropBox. Expectations that work-related materials should not be transmitted over non-managed cloud services is a critical part of the policy.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: Persons are not permitted to transmit, store, or use unapproved cloud services in any way. All persons are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secured in approved cloud storage vendors.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Cloud Services Policy, Axxcess Password Policy and Procedure Manual all outline strict rules for monitoring all data in and out of the network; this applies to all methods and devices used to access client data from inside or outside Axxcess systems. The following are cloud services that are currently approved for use for client data:

- Citrix Sharefile is the only approved Cloud client file storage medium approved for Axxcess' books and records. Any documents responsive to SEC books and records requirements must at all times be kept in Sharefile. This includes client custodial documents, suitability, forms, agreements, applications, authorizations, and trade logs. There are no exceptions to this policy.
- Approved vendors for client data, but not part of Axxcess books and records retention requirements include approved portfolio accounting software: Orion Advisor Tech, financial planning software such as Emoney, Moneyguide Pro, and Advizr, and investment analytical software systems such as Morningstar, Hidden Levers, and Riskalyze, and the Axxcess Allocator.
- Approved cloud storage of client notes and data include both Redtail and Zoho.
- Approved cloud email provider is Redtail Technology. Office 365 is approvable on an exception basis. In no case is any other email provider approved to conduct any business.
- All cloud storage approved vendors must at minimum be accessed via multi factor authentication (MFA) on any device.
- Document or client vaults: Orion Advisor Tech, and Emoney are approved client vaults.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

Encryption Policy:

BACKGROUND: Encryption Policy: This policy defines the requirements for establishing the encryption implementation and management requirements related to the firm computer and communications systems infrastructure. Axxcess has defined places within the firm infrastructure where encryption is warranted, such as laptops, email, Client and employee data, HR data, and other places where critical or otherwise sensitive data is stored.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: Persons are not permitted to maintain client data on any device locally without full data/disk encryption. Full disk encryption must be maintained continuously. Laptops must be shut down after use. You must not download and store any client data locally on any device of any kind outside of permitted systems such as sharefile.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Encryption Policy, and Procedure Manual all outline strict rules for encrypting all data in and out of the network; this applies to all methods and devices used to access client data from inside or outside Axxcess systems. The following are encryption services that are currently approved for use for client data:

- Eset Full Disk Encryption: Eset is provided to you for up to 2 (two) devices. A required license cost determined annually (currently $75) for each device used to store or access client data is required. There are no other encryption services that are currently approved for use.
- Portable devices used to access client data must also have a remote wipe feature enabled.
- Portable devices used to access client data must have geo-location services active.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

Mobile Device Policy:

BACKGROUND: Mobile Device Policy Mobile devices are assets that the firm utilizes on an everyday basis. This policy determines the information security requirements for the protection of sensitive information while being transmitted or received over any type of mobile device. Axxcess mobile device policy details how mobile devices are used and managed. Password and access controls are critical. Mobile app installations guidelines and mobile device wiping and reset guidelines are essential to understand. These include but are not limited to features of Mobile Device Management (MDM), encryption, password expiry, content filtering, whitelisting, and more. Moreover, each class of data available to the device should be defined and policies around it enforced (i.e., Exchange sync, mobile app, emails, etc.).

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: Persons are not permitted to maintain client data on any mobile device. Mobile devices should only be used to access approved cloud services. Mobile devices should always include full data/disk encryption. Full disk encryption must be maintained continuously. Emails accessed on mobile devices must not be stored on mobile devices. Downloads of client data on mobile devices are not permitted. Mobile devices must be bio-metrically secured with either a fingerprint, or facial recognition. Contact management must be limited on mobile devices. You are not permitted to store client data such as dates of birth, SS, or account numbers, or any personally identifiable information (PII) on mobile devices. Your mobile device must include geo location and remote wipe features. You must not share a mobile device with anyone that can access client data.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Encryption Policy, and Procedure Manual all outline strict rules for encrypting all data in and out of the network; this applies to all methods and devices used to access client data from inside or outside Axxcess systems. The following are encryption services that are currently approved for use for client data:

- Guide to Apple IOS mobile security: https://support.apple.com/guide/security/welcome/web
- Android Devices must use: Eset Mobile Security: Eset is recommended for Android devices. Eset Mobile Security provides a bio metric layer of security to each application used on your mobile device.
- Mobile devices used to access client data must also have a remote wipe feature enabled.
- Mobile devices used to access client data must have geo-location services active.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

Password Policy:

BACKGROUND: Password Management Policy: Passwords are the primary token used to access firm information systems. How passwords should be handled must be properly coordinated and supported. Axxcess outlines the specifics on how passwords should be managed by each advisor/employee. Understanding the Password policy is central to staying secure and compliant. Password policies describe how user passwords are created and managed. Include definitions on acceptable password characteristics such as password length, complexity, and a password-change schedule.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action

selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: Passwords must be a minimum of 8 characters, one upper case and one symbol, and must be reset every 90 days. Where possible, multifactor authentication or biometric validation is required. Axxcess will, from time to time review this minimum standard. Persons will access business applications storing client data or other business sensitive information using a password vault/password locker. Axxcess has determined that LastPass Enterprise will used company wide to enforce this global password policy, and implement stricter security procedures when accessing business sites. The following sites are required to be used on Last Pass with exceptions for sites that have MFA implemented (custodians such as Schwab etc):

Sharefile (sharefile.com/Axxcess.sharefile.com/companyname.sharefile.com)
Orion
Zoho
Axxcess Allocator
PandaDoc (CLM)
Financial Planning Sites: Emoney

Download the Last Pass Browser Extension
Download the MFA Authenticator for Last Pass
You will be prompted to use the Last Pass MFA Authenticator upon login.

Users: Click on the invite email and click “Activate”
Activation Code will be sent via Email. Enter the code.
Create a new master password for your last pass account.
Password Policy is enforced- 1 Upper case, 1 digit, 1 special character
Install the Last Pass extension
Enable Last Pass MFA
You will get an email with a QR code to scan on your phone to activate the MFA app.
Clear your google password manager

Sites and applications that contain client data should only be accessed through passwords stored in last pass. Mobile devices should always include MFA to access mobile sites with client data.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Password Policy, and Procedure Manual all outline strict rules for encrypting all password data in and out of the network; this applies to all methods and devices used to access client data from inside or outside Axxcess systems. Passwords must never be shared with anyone. You may not, under any circumstances accept a user name or password from a client or any third party. You are strictly forbidden from using any client or third party credentials to access any applications or sites. This includes banking, real estate, diligence, retirement, or any other site with credentials that are not your own. You must only use credentials and passwords that are issued to you individually. There is no license you hold, or rule available to you that permits you to impersonate a client or prospect. There is no authorization you can accept that accommodates logging in with any credential other than your own.

VIOLATIONS: Violations of securities laws, or violations of company policy due to misuse of password policies will be met with sanction, fine, or termination.

Removable Media Policy:

BACKGROUND: Removable Media Policy This policy defines the requirements for the proper handling of all media that contains firm information. In most organizations, information is generated and stored on many different types of media including paper documents, computer media, and a myriad of portable devices. Much of this information is considered confidential or sensitive, which requires that its handling is performed in a safe and secure manner. The removable media policy should detail how the firm and firm member handle removable media such as USB drives and DVDs or CDs. Consider creating statements that restrict or control the use of USB thumb drives.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action

selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: Client data stored on removable devices such as USB or removable drives is strictly not permitted. This includes presentations, statements, financial reports, and any data or file that has any client personally identifiable data.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Removable Media Policy, and Procedure Manual all outline strict rules for preventing files or data containing any client data saved on removable media in and out of the network; this applies to all methods of saving or storing and all devices used to access client data from inside or outside Axxcess systems.

VIOLATIONS: Violations of securities laws, or violations of company policy due to misuse of password policies will be met with sanction, fine, or termination.

Social Media Policy

BACKGROUND: Social Media Policy Social Media is a predominant part of popular culture and becoming an integral part of business. Firms use social media as means to advertise and keep in touch with clients. Firm policy statements on social media should protect the firm from the dissemination of sensitive information and/or damaging the firm’s reputation.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess. Assets include but not limited to, workstations, servers, mobile phones, software, data, images or text owned, leased, or utilized by Axxcess.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

AXXCESS
WEALTH MANAGEMENT

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER Director

EFFECTIVE DATE (Determined by Director)

REVIEW DATE Annual Review

POLICY STATEMENTS: Axxcess requires that all business related Social Media comply with SEC and Finra regulations regarding Advertising and marketing. As such you are responsible for being familiar with, and complying at all times with the relevant and evolving guidelines for social media use. Any business related correspondence that is conducted on personal social media is strictly forbidden, unless prior approval is provided by Axxcess in writing and that Social Media site under which there is any mention of anything business related must be archived by Global Relay. This includes prospecting, advertising, marketing, and anything communication that could remotely be connected to the business of financial services that occurs on any social media platform. Personal Social Media platforms that are strictly used for personal use must not be used for any business related communication of any kind. Axxcess recognizes that employees may have personal l accounts on a variety of Web-based email accounts such as Facebook, Linkdin, Instagram and others. Axxcess understands that employees may want to use those accounts during work utilizing the personal devices or company assets. It is approved to use personal email on company assets only if used for personal use. Personal use of email should be reserved during non business periods.

Social Media Policy – Any electronic communication with a client or prospect must exclusively be conducted on approved social media platforms. There is a zero tolerance policy for conducting any communication with a client or prospect on personal, non-approved platforms. If such communication occurs inbound from a client or prospect on personal direct messages, inmail, of facebook messenger, whatsapp, or other non approved communication, supervised persons must immediately forward that email to the approved business account and ensure that future correspondence occur on the business account. Axxcess users and approved Axxcess DBAs shall have no expectation of privacy in regards to information that they input or review while using approved Social Media platforms, this includes information on the sender, subject, content, or other information that is entered or transmitted from any device.

Axxcess Code of Ethics, and Axxcess Policy and Procedure Manual all outline strict rules for monitoring all data in and out of the network; this applies to all email accessed from inside or outside Axxcess systems.

Social Media Communications – You must conduct yourself professionally at all times, avoiding using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, members, associates or competitors, or that might constitute harassment or bullying. Axxcess expects all users to act in a morally exemplary manner wherever they may express themselves. Examples of in-appropriate conduct include offensive communication meant to intentionally harm someone’s reputation or communication that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or company policy.

Sensitive Information on Social Media – You must maintain the confidentiality of Client data, account information, and comply at all times with company policy as well as securities laws regarding safe guarding of customer data, advertising and marketing. You must at all times protect private or confidential information. You must protect methods and internal processes and Trade secrets may include information regarding the development of systems, processes, products, know-how and technology. Do not post internal reports, policies, procedures or other internal business-related confidential communications through Social Media, or any other system not approved by Compliance.

Company Opinions - Express only your professional opinions. Never represent yourself as a spokesperson for Axxcess.

Social Media Advertising – Any Social Media post must be submitted for approval prior to sending at hub.axxcessplatform.com/marketing upload. Only approved content may be sent.

EXCEPTIONS: You main submit for approval business related Social Media Sites which will be subject to review, approval and monitoring.

VIOLATIONS: Violations of securities laws, or violations of company policy due to lack of prior approval of business related marketing or advertising will be met with sanction, fine, or termination.

Wireless Communication Policy

BACKGROUND:

Wireless Communication Policy Firm members are constantly part of a connected world. This policy addresses the use of mobile communication devices via wireless communication either Wi-Fi internet or Bluetooth for business purposes – and methods for securing the communicated information. This policy should describe how the firm protects its assets from unauthorized access over Wi-Fi and other wireless vectors. Statements should include the firm's position on personal hotspots and use of guest networks.

SCOPE: This policy applies to the entire Axxcess team, including the CEO, Director, employees, advisors, temporary employees, interns, contractors, sub-contractors, and their respective facilities supporting any operation that interfaces in any way with Axxcess, as well as volunteers and guests who have access to Axxcess assets. Assets include but not limited to, workstations, servers, mobile phones, tablets, and any device used to access the internet for business or personal use.

DEFINITIONS: Policy – A policy is a governing set of principles that guide Axxcess practices. It helps ensure compliance with applicable laws and regulations, promotes operation efficiencies, enhances our culture and values, and reduces organizational risks and above all protects client data. It has broad application throughout Axxcess. It provides a basis for consistent decision making and resource allocation, or a method or course of action

selected to guide and determine, present, and future decisions. It mandates actions or constraints and contains procedures to follow.

COORDINATOR / POLICY AUTHOR Security & Compliance Officer

AUTHORIZING OFFICER; CEO

EFFECTIVE DATE: Immediately and ongoing indefinitely.

REVIEW DATE Ongoing, unnuanced audits and testing.

POLICY STATEMENTS: You should not access client data through any public un protected networks. Examples of public unsecured networks include coffee shops, airports, and other hot spots where the security of the network cannot be verified.

Privacy - Axxcess users shall have no expectation of privacy in regards to information that they input or review while using company assets in regards to devices used to access client data or perform company business, this includes passwords, codes or other information that is entered on any company asset.

Wireless network policy, and Procedure Manual all outline strict rules for preventing files or data containing any client data saved on removable media in and out of the network; this applies to all methods of saving or storing and all devices used to access client data from inside or outside Axxcess systems.

VIOLATIONS: Violations of securities laws, or violations of company policy due to misuse of password policies will be met with sanction, fine, or termination.