Fulcrum Equity Management, LLC
Cybersecurity Policy

Revision Date 01/01/2020

Background

Fulcrum Equity Management, LLC's ("FulcrumEQ") intentions for publishing this Cyber Security Policy is not to impose restrictions that are contrary to our established culture of openness, trust and integrity. FulcrumEQ is committed to protecting our employees, partners, clients 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, internet browsing, and FTP, are the property of FulcrumEQ. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

Purpose

The purpose of this policy and procedure is to ensure the security and confidentiality of our customers' information; protect against any anticipated threats or hazards to the security or integrity of our customers' information; protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any of our customers.

In addition, we will provide the necessary administrative, technical and physical safeguards to assist employees in maintaining the confidentiality of client information. All information, whether relating to a current or former client, is subject to these policies and procedures. Any doubts about the confidentiality of client information must be resolved in favor of confidentiality.

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

This policy applies to employees, contractors, consultants, temporaries, and other workers at FulcrumEQ, including all personnel affiliated with third parties (collectively referred to simple as employees in the remainder of this document). This policy applies to all equipment that is owned or leased by FulcrumEQ.

Action Plans

The firm will identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems; assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

Action Steps

The CCO, or his/her designee, will be responsible for:

- initial implementation of the plan;
- training of employees;
- regular testing of the controls and safeguards established by the plan;
- evaluating the ability of prospective service providers to maintain appropriate information security practices, ensuring that such providers are required to comply with this information security plan, and monitoring such providers for compliance herewith; and
- periodically evaluating and adjusting the plan, as necessary, considering relevant changes in technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to our own business (such as mergers or acquisitions or outsourcing), and/or changes to customer information systems.

Responsibility

The Chief Compliance Officer or his/her designee is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting the firm's client privacy and information protection goals. He/she is responsible for distributing these policies and procedures to employees and conducting appropriate employee training to ensure employee and vendor adherence.

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of Information Resources access privileges, civil, and criminal prosecution.

Risks

The Chief Compliance Officer and his/her designee is responsible for determining reasonably foreseeable internal threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks. See Internal Threat Risk Assessment included in Appendix A.

The Chief Compliance Officer and his/her designee is responsible for determining reasonably foreseeable external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks. See External Threat Risk Assessment included in Appendix B.

Procedure

The Adviser has adopted various procedures to implement the firm's policy and reviews to monitor and ensure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- Hiring Policies and Procedures: Background checks on all employees and any interns or temps and mandatory signing of Employee NDA document to safeguard client information.
- User Account Administration: The Chief Compliance Officer or his/her designee will manage the issuance of all users for the firm. The individual users will select their password for the systems. Upon termination, all user names will be deactivated to remove access.
- Incident Reports: Any suspected breaches in protocol or other issues are to be reported to him/her immediately either via email or phone. This report should include all information regarding users, issues, breaches, etc.
- Facilities: All facilities are always kept locked. No documentation will be left out unattended. All paperwork is to be scanned into secure electronic storage and the originals shredded.
- Vendor Access: FulcrumEQ will segregate sensitive network resources from resources accessible to third parties.

Account Management

- All accounts created must have an associated request and approval that is appropriate for the FulcrumEQ system or service.
- All users must attest to being provided a copy of the FulcrumEQ policies and procedures prior to being given account access.
- All user accounts must have a unique identifier.
- All passwords for accounts must be constructed in accordance with the FulcrumEQ Password Policy.
- All accounts must have a password expiration that complies with the FulcrumEQ Password Policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- System Administrators or other designated staff:
    - Are responsible for creating accounts;
    - Are responsible for removing the accounts of individuals that change roles within FulcrumEQ or are separated from their relationship with FulcrumEQ;
    - Must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes;
    - Must have a documented process for periodically reviewing existing accounts for validity;
    - Are subject to independent audit review;
    - Must provide a list of accounts for the systems they administer when requested by authorized FulcrumEQ management; and
    - Must cooperate with authorized FulcrumEQ management investigating security incidents

Change Management

- Security patches on all systems must be implemented within the specified timeframe of notification from FulcrumEQ.
- Every change to an Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy.
- The CCO may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back-out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.
- Vendor notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Policy.
- A change review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log must be maintained for all changes. The log must contain, but is not limited to:
    - Date of submission and date of change
    - Owner contact information
    - Nature of the change
    - Indication of success or failure
- All information systems must comply with an Information Resources change management process that meets the standards outlined above.

Security Monitoring

- Automated tools will provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible a security baseline will be developed, and the tools will report exceptions. These tools will be deployed to monitor:
    - Internet traffic
    - Email traffic
    - LAN traffic, protocols, and device inventory
    - Operating system security parameters
- The following files will be checked for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
    - Automated intrusion detection system logs
    - Firewall logs
    - User account logs
    - Network scanning logs
    - System error logs
    - Application logs
    - Data backup and recovery logs
    - Help desk trouble tickets
    - Telephone activity – Call Detail Reports
    - Network printer and fax logs

- The following checks will be performed at least annually by assigned individuals:
    - Password strength
    - Unauthorized network devices
    - Unauthorized personal web servers
    - Unsecured sharing of devices
    - Unauthorized modem use
    - Operating System and Software Licenses
- Any security issues discovered will be reported to the ISO for follow-up investigation.

Security Training

- All users must sign an acknowledgement stating they have read and understand FulcrumEQ requirements regarding computer security policies and procedures.
- All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect FulcrumEQ information resources.
- The CCO must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

Vendor Access

- Vendors must comply with all applicable FulcrumEQ policies, practice standards and agreements, including, but not limited to:
    - Safety Policies
    - Privacy Policies
    - Physical Security Policies
    - Auditing Policies
    - Software Licensing Policies
- Vendors must comply with all applicable FulcrumEQ cybersecurity policies, practice standards and agreements, including, but not limited to:
    - Acceptable Use Policies
    - Network Access Policies
- Vendor agreements and contracts must specify:
    - The FulcrumEQ information the vendor should have access to
    - How FulcrumEQ information is to be protected by the vendor
    - Acceptable methods for the return, destruction or disposal of FulcrumEQ information in the vendor's possession at the end of the contract
    - The Vendor must only use FulcrumEQ information and Information Resources for the business agreement
    - Any other FulcrumEQ information acquired by the vendor during the contract cannot be used for the vendor's own purposes or divulged to others
- FulcrumEQ will provide a point of contact for the Vendor. The point of contact will work with the Vendor to confirm the Vendor follows these policies.
- Each vendor must provide FulcrumEQ with a list of all employees working on the contract. The list must be updated and provided to FulcrumEQ within 24 hours of staff changes.

- Each on-site vendor employee must acquire a FulcrumEQ identification badge that will be displayed always while on FulcrumEQ premises. The badge must be returned to FulcrumEQ when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to FulcrumEQ sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate FulcrumEQ personnel.
- If vendor management is involved in FulcrumEQ security incident management the responsibilities and details must be specified in the contract.
    - Vendor must follow all applicable FulcrumEQ change control processes and procedures.
    - Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate FulcrumEQ management.
    - All vendor maintenance equipment on the FulcrumEQ network that connects to the outside world via the network, telephone line, or leased line, and all FulcrumEQ IR vendor accounts will remain disabled except when in use for authorized maintenance.
    - Vendor access must be uniquely identifiable and password management must comply with the FulcrumEQ Password Management Policy. Vendor's major work activities must be entered into a log and available to FulcrumEQ management 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.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to FulcrumEQ or destroyed within 24 hours.
- Upon termination of contract or at the request of FulcrumEQ, the vendor will return or destroy all FulcrumEQ information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of FulcrumEQ, the vendor must surrender all FulcrumEQ identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized FulcrumEQ management.
- All software used by the vendor in providing service to FulcrumEQ must be properly inventoried and licensed.

Non-Disclosure of Client Information

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.

Safeguarding and Disposal of Client Information

The firm restricts access to client information to those employees who need to know such information to provide services to our clients. Any employee who is authorized to have access to client information is required to keep such information in a secure compartment or receptacle on a daily basis as of the close of business each day. All electronic or computer files containing such information shall be password secured and firewall protected from access by unauthorized persons. Any conversations involving client information, if appropriate at all, must be conducted by employees in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of the firm that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures.

Examples of important safeguarding standards that the firm adopted include:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means (e.g. requiring employee use of user ID numbers and passwords, etc.);
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals (e.g. intruder detection devices, use of fire and burglar resistant storage devices);
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- Procedures designed to ensure that customer information system modifications are consistent with the firm's information security program (e.g. independent approval and periodic audits of system modifications);
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information (e.g. require data entry to be reviewed for accuracy by personnel not involved in its preparation; adjustments and correction of master records should be reviewed and approved by personnel other than those approving routine transactions, etc.);
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems (e.g. data should be auditable for detection of loss and accidental and intentional manipulation);
- Response programs that specify actions to be taken when the firm suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies;
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures (e.g. use of fire resistant storage facilities and vaults; backup and store off site key data to ensure proper recovery);
- All mobile and computing devices that connect to applications or resources used by the firm must comply with the Cyber Security 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. Employees must lock the screen or log off when the device is unattended
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware;
- Employees must use extreme caution when installing updates or other software and should attempt to verify the legitimacy of it in advance. Many viruses and malware writers will try to trick the user into thinking the update/software is from a legitimate source when it is not ; and
- Everyone has the responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

For security and network maintenance purposes, authorized individuals within FulcrumEQ may monitor equipment, systems and network traffic at any time;
FulcrumEQ reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy

Acceptable Use

- Users must report any weaknesses in FulcrumEQ computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management.
- Users must not attempt to access any data or programs contained on FulcrumEQ systems for which they do not have authorization or explicit consent.
- Users must not share their FulcrumEQ account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
- Users must not make unauthorized copies of copyrighted software.
- Users must not use any software without FulcrumEQ Information Resources management approval. See Change Management Policy.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources; deprive an authorized FulcrumEQ user access to a FulcrumEQ resource; obtain extra resources beyond those allocated; circumvent FulcrumEQ computer security measures.
- Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, FulcrumEQ users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on FulcrumEQ Information Resources. FulcrumEQ Information Resources must not be used for personal benefit.
- Users must not intentionally access, create, store or transmit material which FulcrumEQ may deem to be offensive, indecent or obscene (other than during academic research where this aspect of the research has the explicit approval of the FulcrumEQ official processes for dealing with academic ethical issues).
- Access to the Internet from a FulcrumEQ owned, home based, computer must adhere to all the same policies that apply to use from within FulcrumEQ facilities. Employees must not allow family members or other non-employees to access FulcrumEQ computer systems.

- Users must not otherwise engage in acts against the aims and purposes of FulcrumEQ as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use

- Incidental personal use of email, internet access, fax machines, printers, copiers, and so on, is restricted to FulcrumEQ approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to FulcrumEQ.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, FulcrumEQ.
- Storage of personal email messages, voice messages, files and documents within FulcrumEQ's Information Resources must be nominal.
- All messages, files and documents – including personal messages, files and documents – located on FulcrumEQ Information Resources are owned by FulcrumEQ, may be subject to open records requests, and may be accessed in accordance with this policy.

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 FulcrumEQ authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing FulcrumEQ 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.

Prohibited System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Accessing data, a server or an account for any purpose other than conducting FulcrumEQ business, even if you have authorized access, is prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- 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.
- 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.

- Circumventing user authentication or security of any host, network or account.
- Providing information about, or lists of, FulcrumEQ clients or employees to parties outside FulcrumEQ.
- Unauthorized use, or forging, of email header information.

Password Guidelines

All passwords should meet or exceed the following guidelines:

- Contain at least 8 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 rabab, 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"

Password Creation

Password creation guidelines are as follows:

- Users must not use the same password for FulcrumEQ accounts as for other non-firm access (for example, personal ISP account, option trading, benefits, and so on).
- Where possible, users must not use the same password for various FulcrumEQ access needs.
- 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

Password changes require the following:

- 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.
- 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.

Password Protection

For password protection purposes:

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- 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.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

Data Backup

All electronic data must be backed-up and recoverable

- 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.
- 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.
- The FulcrumEQ Information Resources backup and recovery process for each system must be documented and periodically reviewed.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems.
- A process must be implemented to verify the success of the FulcrumEQ electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Employees approved for access to FulcrumEQ backup media held by the offsite backup storage vendor(s) must be reviewed annually or when an authorized individual leaves FulcrumEQ.

Disposal

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, and other storage media may contain sensitive data. To protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not sufficient. When deleting files, or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Some methods of disposal to ensure that the information cannot practicably be read or reconstructed that the firm may adopt include:

- Procedures requiring the burning, pulverizing, or shredding or papers containing client information;
- Procedures to ensure the destruction or erasure of electronic media; and
- All data shall be removed from equipment using disk sanitizing software that cleans the media overwriting each disk sector of the machine with zero-filled blocks.
- All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- After due diligence, contracting with a service provider engaged in the business of record destruction, to provide such services in a manner consistent with the disposal rule.
- When Technology assets have reached the end of their useful life they should be sent out for proper disposal.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.
- No computer or technology equipment may be sold to any individual.
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, backup tapes, etc.

Internet Use Filtering System

The FulcrumEQ may block access to Internet websites and protocols that are deemed inappropriate for the firm. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging (except specific applications when approved by the firm)
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web Based Email

Laptops, Cell phones and Tablets

Any FulcrumEQ data stored on a laptop, cell phone or tablet must be saved to an encrypted file system using firm approved software.

Files containing confidential or sensitive data may not be stored on a cell phone or tablet unless protected by approved encryption.

Laptops must employ full disk encryption with an approved software encryption package. No FulcrumEQ data may exist on a laptop in plaintext.

Confidential or sensitive data shall never be stored on personal laptops or computers. Lost or stolen equipment must immediately be reported.

Anti-Virus Guidelines

Recommended processes to prevent virus problems:

- Always run the standard, supported anti-virus software. Download and run the current version; download and install anti-virus software updates as they become available.
- New viruses are discovered almost every day. Perform regular updates.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying them from your Trash.
- Delete spam, chain, and other junk email without forwarding.
- Unsubscribe from any non-business related email sources.
- Never download files from unknown or suspicious sources.
- Examine requests to update software or install new software for legitimacy and don't just click to install without looking. Many virus and malware writers "trick" users into installing their software by attempting to look legitimate.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

Wireless Access

All wireless infrastructure devices must:

- Be installed, supported, and maintained by an approved person.
- Use approved authentication protocols and infrastructure.
- Use approved encryption protocols.
- Maintain a hardware address that can be registered and tracked.

The Adviser's server is not accessible through Wi-Fi access.

Remote Access

FulcrumEQ provides mechanisms to collaborate between internal users, with external partners, and from non-firm systems. All remote access tools or systems that allow communication to FulcrumEQ resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.

Routers

Every router must meet the following configuration standards:

- No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentications.
- The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
- The following services or features must be disabled:
    - IP directed broadcasts
    - Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    - TCP small services
    - UDP small services
    - All source routing and switching
    - All web services running on router
    - Cisco discovery protocol on Internet connected interfaces
    - Telnet, FTP, and HTTP services
    - Auto-configuration
- The following services should be disabled unless a business justification is provided:
    - Cisco discovery protocol and other discovery protocols
    - Dynamic trunking
    - Scripting environments, such as the TCL shell
- The following services must be configured:
    - Password-encryption
    - NTP configured to a corporate standard source
- All routing updates shall be done using secure routing updates.
- Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- Access control lists for transiting the device are to be added as business needs arise.
- The router must be included in the corporate enterprise management system with a designated point of contact.
- Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
- The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    - IP access list accounting
    - Device logging

- Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
- Router console and modem access must be restricted by additional security controls

Periodic Cyber Security Assessments

The firm will conduct periodic assessments (at least annually) to detect potential systems vulnerabilities and to ensure that cybersecurity procedures and systems are effective in protecting confidential customer information. The firm will then respond to deficiencies detected through such assessments by taking timely corrective action in response to detected deficiencies.

Response to Cyber Security Incidents

The firm will respond to data breaches depending on the type and severity of the incident. In doing so, the firm 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