Cybersecurity Policy (CSP)

Ver 1.0.0.1

VantagePointe Financial Group
October 1, 2019

Created By
entreda

Document History and Distribution

Revision History

Revision #	Revision Date	Description of Change	Author
1	October 1, 2019	Initial draft of document	Entreda

Distribution

Recipient Name, Title	Recipient Email	Recipient Organization	Distribution Method
Troy Ernzer, Alison Gillhespy, Executive Vice president	ternzer@vpfgroup.com	VantagePointe Financial Group	Email, Unify Dashboard

CONTENTS

1. BACKGROUND

Living in the information age, we benefit from the increased productivity and efficiencies of using computers and technology. The need for security is apparent, but the need for an Information Security Management Program can be even more important to companies in the computer age. The purpose of such a program is to provide a sustainable and a consistent approach to security that can be replicated time and again across networks, applications, and transactions.

This process begins with a designated individual who oversees and implements the cybersecurity program and enforces the cybersecurity policy. This is an iterative process where risk is assessed, security requirements are defined and solutions are devised to address the identified areas of risk. The organization is responsible for implementing and operating within the boundaries of these security solutions.

The Cybersecurity Policy provides the following general accepted principles and practices for securing information systems. These include -

- Personal computing devices such as laptops and desktop computers
- Mobile devices including mobile phones and tablets
- Server and Datacenter infrastructure including Application, Web, and File Servers
- Network devices including firewalls, switches, routers and load-balancers
- Network office environment which uses business tools and applications and is supported both in an internal and external work environment

1.1 Purpose

This Cybersecurity Policy has been established to address the following:

- Comply with all applicable laws and regulations designed to protect non-public personal information to:

  (a) Ensure the security and confidentiality of Private Information in a manner consistent with SEC/FINRA standards and as required by applicable state law;

  (b) Protect against any anticipated threats or hazards to the security or integrity of the Private Information; and

  (c) Protect against unauthorized access to or use of the Private Information that could result in substantial risk of harm or inconvenience to any Protected Person.

- Establishes responsibilities for protecting VantagePointe Financial Group information assets relating to computer-stored and processing data, computer equipment, and computer software;

- Provides for the implementation of adequate security measures for preventing misuse and loss of VantagePointe Financial Group information assets;

- Establishes the basis for audits and risk assessments, and for preserving management options and legal remedies in the event of information asset loss or misuse;
- Establishes Cyber Security Awareness training as needed to educate, train, and professionalize the workforce in Information Assurance, knowledge, skills, and abilities. Subsequent training to Application and Data Owners, include information systems security, as well as the additional measures and controls to protect information and information systems upon which information is processed, stored, and transmitted against denial of service, unauthorized disclosure (accidental or intentional), modification, or destruction; and
- This policy applies to all regular full-time, regular part-time employees, contractors, consultants, and temporary employees.
- Inventory of all systems and assets is included in Appendix A.

1.2 Security Policy Acknowledgement

All VantagePointe Financial Group employees will receive a copy of the Corporate Cybersecurity Policy. The designated individual is responsible to ensure employees read, acknowledge that they have read, understand and will comply with the Cybersecurity Policy. Updates of the Cybersecurity Policy will be sent to all employees at least on an annual basis.

2. CLASSIFICATION OF INFORMATION

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The company shall classify the information controlled by them.

2.1 Classification of Computer Systems

Here is an example framework for classifying systems :

Security Level	Description	Example
RED	This system contains confidential information – information that cannot be revealed to personnel outside of the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access Server and application(s). Management workstations used by systems and network administrators.
WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
BLACK	This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public Web server with non-sensitive information.

2.2 Network Device Classifications

Network Devices will be classified by the systems directly connected to it.

For example, if a LAN contains just one RED system and all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest-level systems attached to it.

3. ROLES AND RESPONSIBILITIES

Effective cybersecurity requires the active support and ongoing participation of executive staff, and all employees and management levels of the organization. Compliance enforcement is critical in ensuring a sound security program.

When roles and responsibilities are assigned, the "separation of duties" concept must be taken into consideration and implemented to minimize conflicts of interest and to ensure the organizations assets are adequately protected. (Lease access privilege.)

3.1 Designated individual

It is the responsibility of the designated individual to implement, maintain, administer and coordinate the effectiveness of the Information Security Policy. Any questions or comments regarding this Policy should be directed to Troy Ernzer, Alison Gillhespy, the designated individual. Following the resignation or removal of the current designated individual, the Firm shall as soon as reasonably practicable appoint another person to serve in this capacity.

3.2 System Administrator

The systems administrators or a designated individual will monitor performance of all data systems, help isolate problems and resolution and perform and verify systems backups. Additional responsibilities include, but are not be limited to:

- Installing only authorized software
- Recovering systems in a secure manner
- Software license validation
- Virus/malware testing
- Response to monitored alert events
- Provide hardware support
- Operating System support
- Application and Security Patching

3.3 Security/Network Administrator

The security/network administrator or a designated individual provides user access to all systems. Responsibilities include, but may not be limited to:

- Authentication Services (user-ID's)
- Authorization services to applications
- Generation and distribution of reports for monitoring access and potential security breaches
- Perform quarterly vulnerability scan of our network. This must be done in a manner that will not adversely affect VantagePointe Financial Group production environment
- Schedule repairs and patches of vulnerable systems
- Review all policy exceptions on a quarterly basis
- Review security logs daily
- Disable and delete unused, unneeded, or expired user accounts
- Assist auditors in performing their annual environmental audits
- Ensure that all VantagePointe Financial Group data security policies are enforced

4. RISK ASSESSMENT

As of the adoption of this Policy, we have identified the following potential risks to the security, confidentiality and integrity of Private Information that could result in the unauthorized disclosure, misuse, alteration, or other compromise of such information:

- Unauthorized access to documents containing Private Information by our personnel, service providers, Protected Persons or third parties;
- Inappropriate use or disclosure of Private Information by personnel, service providers, Protected Persons or third parties who are authorized to have access to Private Information;
- General security risks posed to our information technology system, including the theft of computers, wireless networks or other equipment permitting access to Private Information, the loss of Private Information due to electrical outages or other computer system failures, and the introduction of viruses into our information technology system; and
- The loss of documents containing Private Information through unanticipated physical hazards such as fire, hurricane, floods or other natural disasters

The designated individual shall periodically re-assess the reasonably foreseeable risks to the security, confidentiality and integrity of Private Information. Such assessment will include analysis of, among other things,

(i) the effectiveness of personnel training and management with regards to the treatment and handling of Private Information

(ii) the reliability and suitability of our information technology systems in light of the objectives of this Policy, including network software design, as well as information processing, storage, transmission and disposal, and

(iii) the ability to detect, prevent and respond to attacks, intrusions or other system failures.

5. LIMITING PRIVATE INFORMATION

VantagePointe Financial Group limits the amount of Private Information collected to that reasonably necessary to accomplish the identified objectives and restricts access to those persons who are required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements. VantagePointe Financial Group restricts user's access to those resources necessary for their business functions.

6. PHYSICAL SECURITY POLICY

Physical security is the primary security layer on which all the other software and hardware security is based. A secure computing and networking environment is impossible to achieve unless appropriate physical security controls are put in place. This policy will seek to address the physical security requirements in all VantagePointe Financial Group managed facilities.

6.1 Locks and Barriers

VantagePointe Financial Group operates in 6 locations. Physical access to every office and work area containing sensitive VantagePointe Financial Group information or live network jacks must be physically restricted. When personnel offices are not being used, computers will be powered off or logged off, to prevent unauthorized access to the network. Private client information will be put away, according to the company's "clean desk" policy. The last person to leave the office each day will lock the office for the evening/weekend.

All information storage media containing sensitive or confidential information must be physically protected and the use of encryption technology is used to protect data against loss. The cage for the T drive will be kept locked at all times. File cabinets will be locked at the end of each business day.

Authorization from VantagePointe Financial Group Security and your manager is required for removal of all computer equipment and computer storage media from the premises. An exception to this policy is the removal of the users' assigned laptop. (Laptops containing sensitive information must use encryption to protect sensitive information.)

6.2 Building Access Records

When a staff member terminates his/her relationship with VantagePointe Financial Group, all physical access codes known to that person shall be changed and all keys, badges and dynamic access tokens must be reclaimed as part of the out processing process.

6.3 Handling Visitors

No visitors will be allowed in the work areas unless they are consultants required to have this access to perform their duties. Their presence and location will be monitored and known at all times.

7. INTERNAL COMPUTER NETWORK CONTROLS

Access to our computer network, including any wireless systems, and any files or programs containing Private Information shall be restricted to only those personnel and service providers who require such access to perform their designated job functions and services. Such controls will include the following:

- We use the Entreda Unify platform to provide support and routine maintenance of the network. The Entreda Unify platform and service functions are designed, among other things, to attempt to report most actual or attempted attacks or intrusions on the network.

- The Entreda Unify platform maintains maps of networks resources, connections and data flows. Entreda Unify will advise the designated individual immediately if there are any breaches to any network connections.

- Virus protection software shall be installed on all computers and monitored by the Entreda Unify platform and will include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

- The computer network and all computers are protected by a firewall. Not less frequently than once during each 12- month period, all operating systems and applications shall be upgraded with any currently available security patches or other security-related enhancements available from the providers of such systems and applications. The Entreda Unify platform is designed to correct non-compliance of the firewall and to alert the 1 regarding any non-compliant systems.

- All access to the computer network and to each computer shall be password protected and other reasonable authentication protocols provided by Entreda, in accordance with industry standards as determined from time to time in consultation with Entreda. Currently passwords are changed for every computer enrolled in the Entreda system every 60 days.

- Following the termination of employment of any of our personnel, all necessary steps shall be taken to prevent such terminated employee from accessing records containing Private Information by, among other things, immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names. All associations with the Entreda Unify Platform can be terminated immediately by an authorized administrator following a termination of an employee. This ensures the employee can no-longer access the firm's systems or have access to the data stored under the employee's user profile in his/her computer.

- To the extent that personnel are supplied with remote access devices, including, without limitation, laptop computers, we shall track such devices and take inventory at least annually.

- Private Information stored on the network shall be backed up on a regular basis and these backups will be verified on a quarterly basis.

- VantagePointe Financial Group takes steps to secure the Private Information that may be stored on laptops or other portable devices, including (as applicable) password protection, data encryption. The Entreda Unify platform continuously monitors, remediates and reports on all enrolled devices for firewall, anti-virus/anti-malware, password protection, data encryption, screen-locks and other cybersecurity best practices.

8. 3RD PARTY SERVICE PROVIDERS

Prior to engaging any third-party service provider who may receive Private Information, we will take appropriate measures to determine whether such service provider maintains sufficient procedures to detect and respond to security breaches, as required by this Policy and applicable law.

If necessary, we may require a prospective service provider to certify to us that it maintains such procedures. Contracts with service providers will contain appropriate provisions to protect the security, confidentiality and integrity of all Private Information that is in their possession. We will undertake to monitor our service providers' compliance with such contractual provisions as well as the service providers' own internal security procedures on a case-by-case basis depending on the sensitivity of any relevant Private Information in their possession.

9. EMPLOYEE MANAGEMENT AND TRAINING

We shall implement appropriate measures to ensure that all personnel are informed of and comply with this Policy. Such measures will include the following:

- Human Resources or individuals responsible for hiring shall check the references and background) of any prospective personnel who may have access to Private Information.
- The designated individual will provide a copy of this Policy to all personnel, each of whom shall agree to comply with its terms and conditions. Each individual who is hired by us as personnel following adoption or amendment of this Policy shall also be required to read and sign a copy of this Policy or the then-current Information Security Policy.
- VantagePointe Financial Group conducts an annual training/refresher class to review the Cybersecurity Policy and identify some of the new threats that are becoming more prevalent to improve the overall awareness of the staff.
- All personnel are instructed to take basic steps to maintain the security, confidentiality and integrity of Private Information, including: locking rooms and file cabinets where paper records are kept; using a password-activated screen saver; using strong passwords; periodically changing passwords (currently no less frequently than on a semi-annual basis); avoiding the transmission of unencrypted Private Information on public networks; and disposing of Private Information in a secure manner; not keeping open files containing Private Information on their desks when they are not at their desks; and securing all physical and electronic files at the end of the work day in a manner consistent with this Policy.
- Disciplinary measures will be imposed for any breaches of this Policy. Such measures could include: verbal counseling, a letter of censure, a suspension (with or without pay), a fine, a demotion or termination of employment. In determining what action is appropriate in a particular case, the company will take into account all relevant information, including the nature and severity of the violation, whether the violation was a single occurrence or repeated occurrences, whether the violation appears to have been intentional or inadvertent, whether the individual in question had been advised prior to the violation as to the proper course of action and whether or not the individual in question had committed other violations in the past. Disciplinary measures will be at the discretion of the designated individual.
- Employees are encouraged to report to the designated individual any suspicious or unauthorized use of Private Information.

10. BREACHES OF SECURITY

The designated individual shall conduct a mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of Private Information following any incident involving a material breach of security. Any information related to possible breach to the end-points, network or the Entreda Unify platform shall be reported to the designated individual. [All such events will be logged for the length of the service and any remediation actions suggested to eliminate or reduce the impact of the breach shall be provided at such time.]

11. ROUTINE TESTING OF CONTROLS, SYSTEMS AND PROCEDURES

The effectiveness of this Policy will be regularly evaluated and tested through the use of audits and operational testing where appropriate. Where possible and appropriate, security procedures will be tested and verified annually in a test or isolated environment. All systems and services provided by the Entreda Unify platform will be routinely audited in an automated fashion and reported to the Firm. Compliance reports are automatically generated by the system so as to report.

A sample report is attached in Appendix A.

12. SECURITY PROGRAM EVALUATION AND ADJUSTMENT

The designated individual will continually monitor, evaluate and adjust this Policy in light of the results of the testing and monitoring of the overall information security program contemplated by this Policy. The designated individual will also evaluate and adjust this Policy as appropriate to address:

(i) The current risk assessment, management and control activities

(ii) Any new risks or vulnerabilities identified by the designated individual using the standards set forth above,

(iii) Any technology changes that may affect the protection of private information,

(iv) Material changes to our business, including the size, scope and type of our business;

(v) The amount of resources available;

(vi) The amount of private information stored or held;

(vii) Any increased need for security and confidentiality of both consumer and employee information; and

(viii) Any other circumstances that the designated individual believes may have a material impact on the information security policy. The designated individual will report the status of this policy, compliance problems (if any) relating thereto and recommendations for improvement thereof. The designated individual will also provide updated information regarding the information security policy to all personnel.

Executed copies of these policies and procedures shall be retained (in original or electronic form) for not less than six years.

Adopted as of _____

13. RECEIPT AND ACKNOWLEDGMENT

The undersigned hereby acknowledges his or her receipt of the VantagePointe Financial Group's Cybersecurity Policy and that he or she has read the Cybersecurity Policy and agrees to comply with its terms and conditions.

_____
(Signature)

_____
(Printed Name)

_____
(Date)

APPENDIX A | REPORTS – SAMPLE

Refer to the Cybersecurity Surveillance Report generated by the Entreda Unify system

Server Report

Server Name	Owner	Administrator	Purpose/Use	IP Address	MAC Address	Date Established	Last Updated	Operating System	O/S Version	Latest Patch	Anti-Virus Software	Password Change Date	Physical/VM/ Cloud
Available	Available	Manual Entry	Manual Entry	Available	Available	?	?	Available	?	Available	Available	?	Manual Entry

Workstation/Laptop Report

Server Name	Owner	Administrator	Purpose	MAC Address	Operating System	Latest Patch	Anti-Virus Software	Password Change Date	Screen Blocking Enabled	Storage Encryption	Office Application Version	PDP Software	Unapproved Cloud Storage
Available	Available	Manual Entry	Manual Entry	Available	Available	Available	Available	Available	?	Available	?	Available	Available

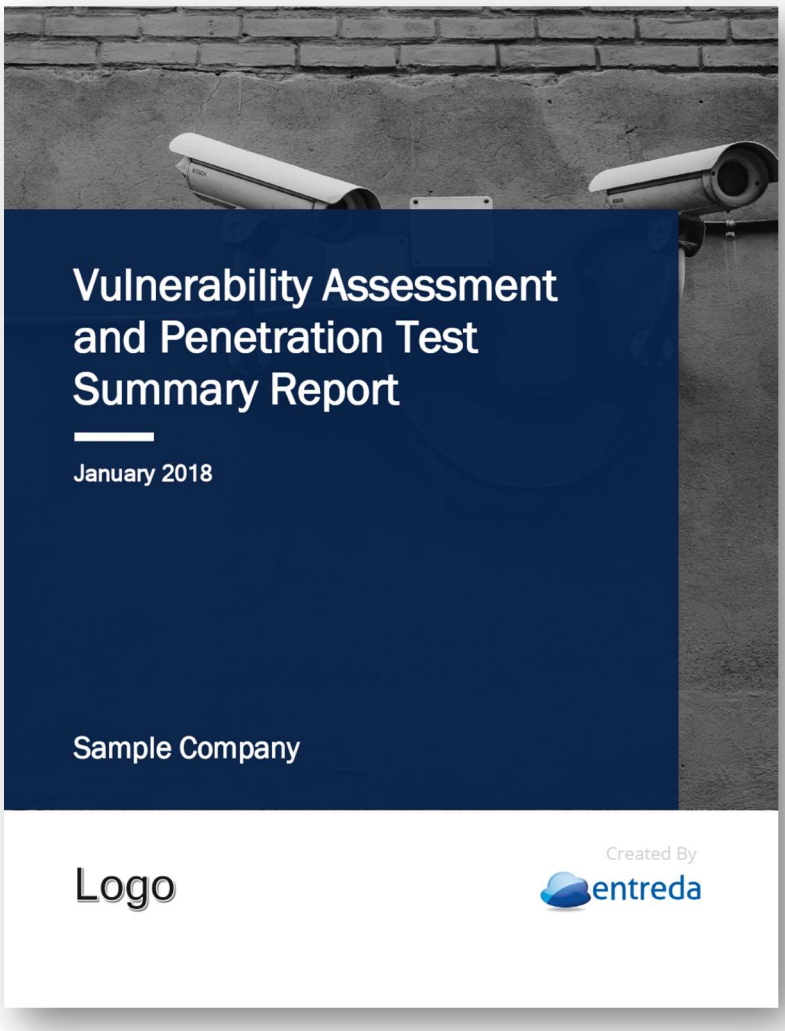
Tablets

User Name	Account Name	Domain Name	Encryption Enabled? (Y/N)	PIN Enabled (Y/N)	Operating System	O/S Version	Exchange Active Sync (PoP3/IMAP4)	MAC Address

Smartphones

User Name	Domain Name	ISMI	IMEI	Encryption Enabled? (Y/N)	PIN Enabled (Y/N)	Operating System	O/S Version	MAC Address

APPENDIX B – VULNERABILITY AND PENETRATION TEST REPORT

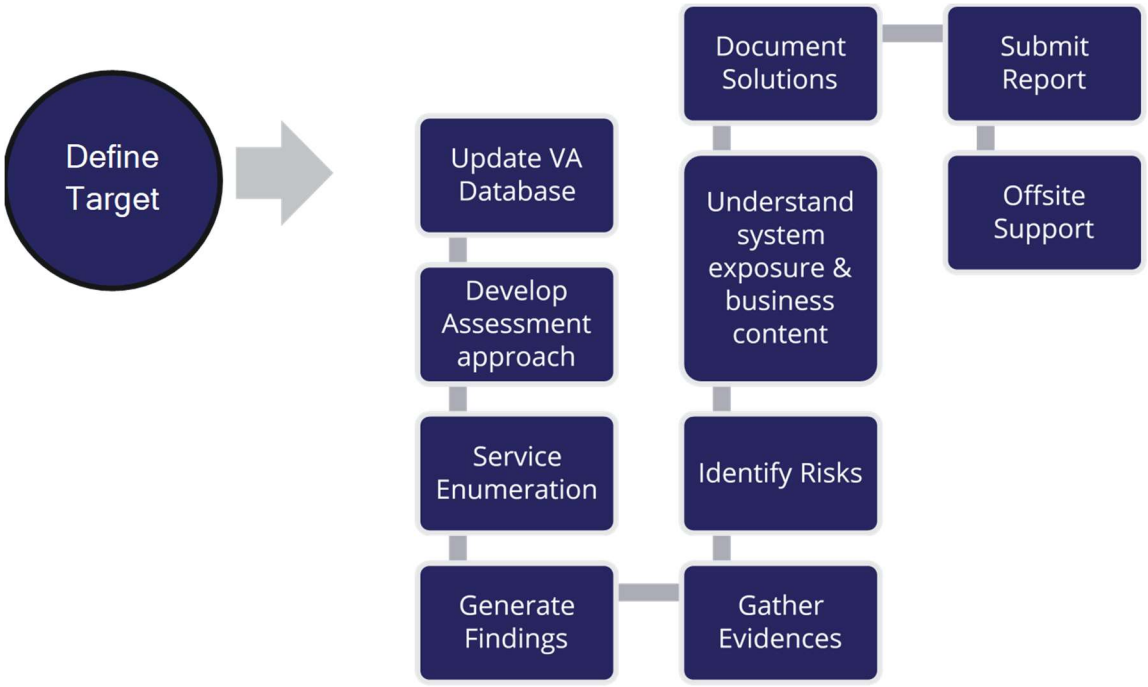


APPENDIX C – RISK ASSESSMENT

The last time a Vulnerability Assessment/Penetration Test was completed was
.

Methodology

Security testing was carried out as per the following methodology. Automated scanning and manual testing was carried out.



Here is a sample list of checks to be done to help establish a security baseline on Websites.

(1) Check if web application is able to identify spam attacks on contact forms used in the website.

(2) Spam email filters – Verify if incoming and outgoing email traffic is filtered and unsolicited emails are blocked.

(3) Firewall – Make sure entire network are protected with an approved Firewall.

(4) Verify that all usernames and passwords are encrypted and transferred over secured connection e.g., https.

(5) Verify information stored in website cookies. It should not be in readable format.

(6) Check previously found vulnerabilities to verify the problem has been mitigated.

(7) Verify there are no open ports in network.

(8) Verify WIFI network security.

(9) Password should be a minimum of 8 characters containing upper and lower case letters, at least one number and one special character.

(10) Username should not be "password", "admin" or "administrator".

(11) Login page should be locked upon (3 to 5) unsuccessful login attempts.

(12) Error messages should be generic and should not mention specific error details like "Invalid username" or "Invalid password".

(13) Verify use of registry entries. Sensitive information should not be kept in registry.

(14) All files must be scanned before uploading to server.

(15) Sensitive data should not be passed in URLs while communicating with different internal modules of the web application.

(16) There should not be any hard coded username or password in the system.

(17) Verify that the reset password functionality is secure.

(18) Verify application for SQL Injection

(19) Verify application for Cross Site Scripting

(20) Critical resources in the system should be available to authorized persons and services only.

(21) All access logs should be maintained with proper access permissions.

(22) Verify user session ends upon log off.

(23) Verify that all applications and database versions are up to date

APPENDIX D – ASSET INVENTORY

Desktops/Laptops	Servers
0	

Printers	Scanners	Fax Machines

Personal Devices

APPENDIX E - POLICY DOCUMENTS

A1. Personal Computer and BYOD Policy

Objective

The objective of this policy is to provide information security instructions applicable to all users (employees, contractors, consultants, temporaries, vendors, etc.) who use VantagePointe Financial Group Personal Devices.

Scope

All VantagePointe Financial Group PC users are expected to comply with this policy. This policy applies whether PC's are stand-alone or connected to the VantagePointe Financial Group network.

Introduction

A large portion of VantagePointe Financial Group business is conducted with PCs (Desktops, laptops, PDA's and similar computers dedicated to a single user's activity). Protection of these PCs and the information handled by these systems is an essential part of doing business at VantagePointe Financial Group.

VantagePointe Financial Group conducts business with 100 devices. These devices are expected to have access to PII data, here is a list of devices:

0

GUIDELINES

- **Business Use Only**: VantagePointe Financial Group information systems must be used only for business purposes. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not preempt any business activity. Examples of unacceptable personal use include game playing, downloading music, downloading illegal software and surfing the Internet for entertainment purposes.

- **Changes to Application Software**: VantagePointe Financial Group has a standard list of permissible software packages that users can run on their PCs. As much as possible, users must not install other software packages on Business Use PCs, MACs or mobile devices without obtaining advance permission from the designated individual. VantagePointe Financial Group utilizes Entreda Unify to inventory all new applications installed on Business Use PCs, MACS and/or mobile devices.

- **Changes to Operating System Configurations**: On Business Use computer hardware, users must not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they will be performed at the direction of the designated individual. VantagePointe Financial Group utilizes Entreda Unify to inventory all new applications installed on Business Use PCs, MACs and/or mobile devices.

- **Access Control**: All VantagePointe Financial Group computers must run an access control package (ie: Screen Saver lockout) approved by the DESIGNATED INDIVIDUAL. Typically these packages require a fixed password at the time a computer is booted and again after a certain period of no activity. Users must set the time frame for this period of no activity -- at which point the contents of the screen are obscured -- to 15 minutes or less. If sensitive information resides on a computer, the screen must immediately be protected with this access control package, or the machine turned off, whenever a worker leaves the location where the PC is in use (for example, when leaving one's desk to go to the coffee machine). VantagePointe Financial Group utilizes Entreda Unify to monitor access control policies on Business Use PCs, MACs and/or mobile devices.

- **Choice and Storage of Passwords**: The user-chosen passwords employed by access control software packages, should follow the guidelines specified in the Password Policy. Users must maintain exclusive control of their personal passwords; they must not share them with others at any time. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access controls, or in any other locations where unauthorized persons might discover them.

- **Corporate Domain Membership**: VantagePointe Financial Group users may join their computers to the corporate domain. This enables all VantagePointe Financial Group computers to be managed and protected. In this scenario, users are not permitted to change administrative privileges on any VantagePointe Financial Group owned computers. IT System Administrators should have administrative access to all VantagePointe Financial Group owned computers.

- **Laptop physical security**: All VantagePointe Financial Group provided laptops must be locked down when left unattended.

- **Anti-Virus Program Installed**: All Microsoft Windows based computers must continuously run the current version of VantagePointe Financial Group approved virus detection package. Users must not abort or uninstall the virus scan program, especially when they are connected in any way to the VantagePointe Financial Group sensitive data. VantagePointe Financial Group utilizes Entreda Unify to monitor anti-virus programs installed on PCs, MACs and/or mobile devices.

- **Decompression before Checking**: Externally supplied media (USB drives, DVD and similar) must not be used unless they have first been checked for viruses. Externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be decompressed (unzipped) prior to being subjected to an approved virus checking process. If the files have been encrypted, they must be decrypted before running a virus-checking program. It is important to note that in some cases, virus-checking programs cannot detect viruses in compressed or encrypted files.

- **Eradicating Viruses**: Because viruses can be complex and sophisticated, any suspected PC virus infection must immediately be reported to the DESIGNATED INDIVIDUAL. If the suspected virus appears to be damaging information or software, users must immediately disconnect from the network.

- **Authoring Viruses**: Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any VantagePointe Financial Group computer system. (Viruses, worms, or a Trojan horses.)

- **Periodic Back-Up**: All sensitive, valuable, or critical information resident on VantagePointe Financial Group computer systems must be periodically backed-up. Such back-up processes must be performed at least weekly. The company has a policy to not store local back-up's and all data with access to PII is stored in the cloud.

- **Copyright Protection**: VantagePointe Financial Group, strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden. Likewise, VantagePointe Financial Group allows reproduction of copyrighted materials only to the extent legally considered "fair use" or with the permission of the author/owner. If users have any questions about the relevance of copyright laws, they should contact the designated individual or corporate legal counsel. Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.

- **Downloading Sensitive Information**: Sensitive VantagePointe Financial Group information may be downloaded from a server to a desktop/laptop computer only after two conditions have been fulfilled. For this data transfer to take place, a clear business need must exist and advance permission from VantagePointe Financial Group must be obtained. This policy is not intended to cover e-mail or memos, but does apply to any sensitive PII data.

- **Tools to Compromise Systems Security**: Unless specifically authorized by the designated individual, users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Unless specific permission has been obtained from the designated individual, users are prohibited from using such tools.

- **Reporting Problems**: Users must promptly report information security alerts, warnings and suspected vulnerabilities to: the Designated individual.

A2. Password Policy

Purpose

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

Scope

This policy applies to all users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any VantagePointe Financial Group facility, has access to the VantagePointe Financial Group network, or stores any non-public VantagePointe Financial Group information.

Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of VantagePointe Financial Group entire corporate network. As such, all VantagePointe Financial Group employees (including contractors and vendors with access to VantagePointe Financial Group systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

General

- All system-level passwords (e.g., root, enable, Windows admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) MUST be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs such as "pseudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

  All user-level and system-level passwords must conform to the guidelines for strong password as described below

GUIDELINES

Poor, weak passwords have the following characteristics:

- The password contains less than seven characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "miami", "sanjose", "sanfran" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least seven alphanumeric characters.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

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

Password Protection Standards

- Do not use the same password for VantagePointe Financial Group accounts as for other non-VantagePointe Financial Group access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various VantagePointe Financial Group access needs. For example, select one password for the financial systems and a separate password for the CRM system. Also, select a separate password to be used for a Windows server account and a Mac account, for instance.

- Do not share VantagePointe Financial Group passwords with anyone, including administrative assistants.

- All passwords are to be treated as sensitive, Confidential VantagePointe Financial Group information.

- Here is a list of "**DON'Ts**":

    - Don't reveal a password over the phone to ANYONE
    - Don't reveal a password in an email message
    - Don't reveal a password to your manager
    - Don't talk about a password in front of others
    - Don't hint at the format of a password (e.g., "my family name")
    - Don't reveal a password on questionnaires or security forms
    - Don't share a password with family members
    - Don't reveal a password to co-workers while on vacation
    - If someone demands a password, refer them to this document.
    - Do not use the "Remember Password" feature of applications (e.g., Outlook, Google and others).
    - Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart phones or tablets) without encryption.
    - Change passwords at least once every six months (except system-level passwords which must be changed quarterly).

- If an account or password is suspected to have been compromised, report the concern to the designated individual and change all passwords.

- The designated individual or delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

- If a senior staff member leaves the VantagePointe Financial Group for any reason, all administrator passwords will be immediately changed.

- It is strongly recommended that all personnel enable auto locking password-protected screensavers on their desktops/laptops to prevent misuse if they are absent from their desks.

A3. Acceptable Use and Internet Policy

Objective

The objective of this policy is to provide cybersecurity instructions applicable to all users (employees, contractors, consultants, temporaries, vendors, etc.) who use VantagePointe Financial Group Internet Resources.

Scope

This policy applies to all users who use the Internet with VantagePointe Financial Group computing or networking resources, as well as those who represent themselves as being connected--in one way or another--with VantagePointe Financial Group. All Internet users are expected to be familiar with and fully comply with this policy.

Introduction

VantagePointe Financial Group provides the use of the Internet as a productivity enhancement tool. VantagePointe Financial Group encourages the business use of the Internet for business related purposes. Occasional use for personal purposes is permitted as long as it does not interfere with business-related functions. The guidelines in this document will outline acceptable and unacceptable uses of VantagePointe Financial Group computing and networking resources.

GUIDELINES

Information Integrity

Information Reliability: All information taken off the Internet should be considered suspect until confirmed by reliable sources. There is no quality control process on the Internet, and a considerable amount of its information is outdated and inaccurate, and in some instances even deliberately misleading. Accordingly, before using Internet-supplied information for business decision-making purposes, users must corroborate the information by consulting other sources.

Virus Checking: All files downloaded from non-VantagePointe Financial Group sources via the Internet must be screened with virus detection software prior to being used in any way. Refer to VantagePointe Financial Group Anti-Virus policy. "Whenever an external provider of the software is not trusted, downloaded software should be tested on a stand-alone non-production machine that has been recently backed-up" If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the test machine. Downloaded files must be decrypted and decompressed before being screened for viruses. Separately, the use of digital signatures or MD5 checksums to verify that unauthorized parties have not altered a file is recommended. While these are prudent steps that should be taken, this still does not assure freedom from viruses and worms.

Spoofing Users: Unless tools like digital signatures and digital certificates are employed, it is relatively easy to spoof the identity of another user on the Internet. Before users release any confidential information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed via digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third party references, and telephone conversations may be used.

User Anonymity: Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any VantagePointe Financial Group system is forbidden. The user name, email address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. Use of anonymous FTP log-ins, HTTP (web) browsing, and other access methods established with the expectation that users would be anonymous are permissible.

Attachments: Users must not open email attachments unless they were expected from a known and trusted sender. Such attachments may include viruses or other malicious software. Hence all attachments, regardless of their source should be scanned using anti-virus software prior to opening. Email clients, such as Microsoft Outlook, which open attachments by default should be configured to disable this behavior.

Web Page Changes: Users may not establish new Internet web pages dealing with VantagePointe Financial Group business, or make modifications to existing web pages dealing with VantagePointe Financial Group business, unless they have first obtained the approval of the Marketing and/ the designated individual. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page. These departments will make sure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected with adequate security measures.

Information Confidentiality

Information Exchange: In keeping with the confidentiality agreements signed by all Users, all VantagePointe Financial Group software, documentation and other internal information must not be sold or otherwise transferred to any non- VantagePointe Financial Group party for any purposes other than business purposes expressly authorized by management. Exchanges of software and/or data between VantagePointe Financial Group and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. Regular business practices--such as shipment of a product in response to a customer purchase order--need not involve such a specific agreement since the terms and conditions are implied.

Posting Materials: Users must not post unencrypted VantagePointe Financial Group material (software, internal memos, policies, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar publicly accessible services, unless Marketing has first approved the posting of these materials. In more general terms, VantagePointe Financial Group internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate business need-to-know the involved information.

Message Interception: Wiretapping and other types of message interception are straightforward and frequently encountered on the Internet. Accordingly, VantagePointe Financial Group confidential, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods. Unless specifically known to be in the public domain, sensitive data must always be

encrypted before being sent over the Internet. Virtual Private Network (VPN) service should be utilized at all times when accessing public hotspots.

Security Parameters: Unless a connection is encrypted, credit card numbers, telephone calling card numbers, fixed login passwords, and other security parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable format. The SSL or AES encryption processes are both acceptable Internet encryption standards for the protection of security parameters. Other encryption processes, such as PGP, are permissible if they are pre-approved by the designated individual or VantagePointe Financial Group's IT manager.

Intellectual Property Rights

Copyrights: VantagePointe Financial Group strongly supports strict adherence to software vendors' license agreements. When at work, or when VantagePointe Financial Group computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Similarly, the reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author/owner. Users should assume that all materials on the Internet are copyrighted unless specific notice states otherwise.

Access Control

Inbound User Authentication: All users wishing to establish a real-time connection with VantagePointe Financial Group internal computers via the Internet must authenticate themselves at a firewall/VPN device before gaining access to VantagePointe Financial Group internal network. This authentication process must be achieved via a password system approved by the designated individual. These systems will prevent intruders from guessing fixed passwords or from replaying a fixed password captured via a "sniffer attack" (wiretap). Designated "public" systems (anonymous ftp, web surfing, etc.) do not need user authentication processes because anonymous interactions are expected.

Browser User Authentication: Users must not save fixed passwords in their web browsers or email clients because this may allow anybody who has physical access to their workstations to both, access the Internet with their identities, as well as read and send their email. Instead, these fixed passwords must be provided each time that a browser or email client is invoked. Browser passwords may be saved if and only if a boot password must be provided each time the computer is powered-up, and if a screen saver password must be provided each time the system is inactive for a specified period of time. Similarly, VantagePointe Financial Group computer users must refuse all offers by software to place a cookie on their computer so that they can automatically login the next time that they visit a particular Internet site.

Establishing Network Connections: Unless the prior written approval of the designated individual has been obtained, Users may not establish Internet or other external network connections that could allow non-VantagePointe Financial Group users to gain access to VantagePointe Financial Group systems and information. These connections include the establishment of Internet web pages, Internet commerce systems, ftp servers, and the like. Sharing your password or user credentials with the intent of providing unauthorized access to VantagePointe Financial Group resources is strictly prohibited. Any such activity will be treated as a malicious attack on VantagePointe Financial Group computing resources.

Personal Use

Personal Use: VantagePointe Financial Group management encourages Users to explore the Internet for business purposes. Incidental personal use is permissible if the use: (a) does not consume more than a trivial amount of resources that could otherwise be used for business purposes, (b) does not preempt any business activity. Examples of unacceptable personal use include game playing, downloading music, downloading illegal software and surfing the Internet for entertainment purposes.

A growing practice on the Internet is the use of peer-to-peer (P2P) file sharing networks (such as BitTorrent, Limewire, eMule, KaZaa, Morpheus, Gnutella, Ares Galaxy, etc.), which involve the unauthorized copying and sharing of copyrighted material with other Internet users. Such illegal activity can be the source of libel, copyright infringement and other legal problems for VantagePointe Financial Group and is strictly prohibited. Use of P2P is against policy.

VantagePointe Financial Group utilizes Entreda Unify to monitor if P2P software installed on any PCs, MACs and mobile devices.

Blocking Sites: VantagePointe Financial Group firewalls may prevent users from connecting with certain non-business web sites. VantagePointe Financial Group computer users who discover they have connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material must immediately disconnect from that site. The ability to connect with a specific web site does not in itself imply that users of VantagePointe Financial Group systems are permitted to visit that site. Users shall not use non-VantagePointe Financial Group resources for the purposes of testing and other business-related purposes without the permission of the owners of such resources.

Privacy

No Default Protection: VantagePointe Financial Group information systems users should realize that their communications over the Internet are not automatically protected from viewing by third parties. Unless encryption is used, Users should not send information over the Internet if they consider it to be confidential or private.

Management Review: At any time and without prior notice, VantagePointe Financial Group management reserves the right to examine e-mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, and other information stored on or passing through VantagePointe Financial Group computers. Such management access assures compliance with internal policies, assists with internal investigations, and assists with the management of VantagePointe Financial Group information systems.

Logging: VantagePointe Financial Group may routinely log web sites visited, files downloaded and related information.

Junk E-mail: Users are prohibited from using VantagePointe Financial Group computer systems for the transmission of unsolicited bulk email advertisements or commercial messages, which are likely to trigger complaints from the recipients. Colloquially known as "spam," these prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches. When Users receive unwanted and unsolicited e-mail (also known as spam), they must

refrain from responding directly to the sender. Instead, they should forward the message to the e-mail administrator at VantagePointe Financial Group who can then take steps to prevent further transmissions and can take steps to contact the offending parties. To respond to the sender would be indicate that the user-ID is monitored regularly, and this would then invite further junk email.

Reporting Security Problems

Notification Process: The DESIGNATED INDIVIDUAL must immediately be notified in the event of the following:

a) If sensitive information is lost, or suspected of being lost or disclosed to unauthorized parties

b) If any unauthorized use of VantagePointe Financial Group information systems has taken place, or is suspected of taking place

c) Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.

Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported to the DESIGNATED INDIVIDUAL. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports: The Internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of chain letters, which request that the receiving party send the message to other people. Users in receipt of such information about system vulnerabilities must forward it to the IT Administrator or Designated individual, who will then determine what if any action is appropriate. Users must not personally redistribute system vulnerability information or post it on any public forum such as the VantagePointe Financial Group bulletin board.

Testing Controls: Users must not "test the doors" (probe) security mechanisms at either VantagePointe Financial Group or other Internet sites unless they have first obtained permission from the DESIGNATED INDIVIDUAL. If Users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity. Likewise, both the possession and the usage of tools for cracking information security (such as SATAN/SAINT, nmap, crack etc) are prohibited without the advance permission of the DESIGNATED INDIVIDUAL.

A4. Electronic Mail Policy

Purpose

The purpose of this policy is to establish a standard for e-mail communication.

Scope

The scope of this policy includes all users who have or are responsible for an e-mail account on any VantagePointe Financial Group-owned and maintained mail system.

Introduction

VantagePointe Financial Group IT provides the use of e-mail as a productivity enhancement tool; VantagePointe Financial Group encourages the business use of e-mail systems (notably the Internet, voice mail, e-mail, and fax). Unless third parties have clearly noted copyrights or some other rights on the messages handled by these e-mail systems, all messages generated on or handled by these systems are considered to be the property of VantagePointe Financial Group.

Guidelines

Authorized Usage: VantagePointe Financial Group e-mail systems generally must be used only for business activities. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of system resources, (b) does not preempt any business activity. This means that VantagePointe Financial Group e-mail systems must not be used for charitable fundraising campaigns, political advocacy efforts, private business activities, or personal amusement and entertainment. On a related note, news feeds, email mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material which is clearly related to VantagePointe Financial Group business purposes. Users are reminded that the use of corporate information system resources should never create either the appearance or the reality of inappropriate use.

Default Privileges: Electronic communication systems must be established and maintained such that only the privileges necessary to perform a job are granted to a user. For example, when a user's relationship with VantagePointe Financial Group comes to an end, all the user's privileges on VantagePointe Financial Group e-mail systems will also come to an immediate end i.e. e-mail will not be forwarded).

User Separation: E-mail systems must employ personal user-IDs and associated passwords to isolate the communications of different users. Users must not employ the user-ID or other identifier of any other user. All generic accounts setup for testing or other purposes should have a clear designated owner. Any changes in the owner's privileges will result in such user-Ids being revoked.

User Accountability: Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user, except for circumstances as authorized and pre-approved by the Designated individual.

User Identity: Misrepresenting, obscuring, suppressing, or replacing another user's identity on an e-mail system is forbidden. The user name, e-mail address, organizational affiliation, and related information included with e-mail messages or postings must reflect the actual originator of the messages or postings. Users must not send anonymous e-mail. At a minimum, all users must provide their name and phone number in all e-mail communication. E-mail "signatures" indicating job title, VantagePointe Financial Group affiliation, address, and other particulars are strongly recommended for all e-mail messages.

Use Only VantagePointe Financial Group E-Mail Systems: Unless approved by VantagePointe Financial Group, users must not use their personal e-mail accounts with an Internet Service Provider (ISP) or any other third party for any VantagePointe Financial Group business messages. To do so would circumvent logging, SPAM control, virus prevention and backup controls that VantagePointe Financial Group has established. Likewise, users must not use the e-mail features found in web browsers for any VantagePointe Financial Group business communications; they must instead employ authorized VantagePointe Financial Group e-mail software. Please see further information in the firm's **Policies and Procedures Manual, section on Electronic Communications.**

Respecting Intellectual Property Rights: Although the Internet is an informal communications environment, the laws for copyrights, patents, trademarks, and the like still apply. To this end, users using VantagePointe Financial Group e-mail systems must (1) repost or reproduce material only after obtaining permission from the source, (2) quote material from other sources only if these other sources are properly identified, and (3) reveal internal VantagePointe Financial Group information on the Internet only if the information has been officially approved by VantagePointe Financial Group for public release.

No Guaranteed Message Privacy: VantagePointe Financial Group cannot guarantee that e-mail will be private. Users should be aware that e-mail can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, e-mail can be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, e-mail may actually be retrievable.

Contents of Messages: Users must not use profanity, obscenities, or derogatory remarks in e-mail messages discussing employees, customers, competitors, or others. Such remarks -- even when made in jest -- may create legal problems such as trade libel and defamation of character. It is possible that such remarks would later be taken out of context and used against VantagePointe Financial Group. As a matter of standard business practice, all VantagePointe Financial Group electronic mail communications must be consistent with conventional standards of ethical and polite conduct.

Incidental Disclosure: It may be necessary for VantagePointe Financial Group to review the content of an individual user's communications during the course of problem resolution.

Harassing or Offensive Materials: VantagePointe Financial Group computer and communications systems are not intended to be used for, and must not be used for the exercise of the users' right to free speech. These systems must not be used as an open forum to discuss VantagePointe Financial Group organizational changes or business policy matters.

Likewise, as a further restriction of free speech, sexual, ethnic, and racial harassment via e-mail is prohibited. Users who receive offensive unsolicited material from outside sources must not forward/redistribute it to either internal or external parties (unless this forwarding/redistribution is to the VantagePointe Financial Group in order to assist with the investigation of a complaint).

Purging E-Mail: Messages no longer needed for business purposes must be periodically purged by users from their e-mail folders. Not only will this increase scarce storage space, it will also simplify records management and related activities.

Public Representations: No media advertisement, Internet home page, electronic bulletin board posting, e-mail message, or any other public representation about VantagePointe Financial Group may be issued unless it has first been approved by the Marketing or Public Relations Departments. If users are bothered by an excessive amount of spam from a particular organization or e-mail address, they must not respond directly to the sender. Users should instead unsubscribe from organization lists.

Message Forwarding: Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, e-mail users should exercise caution when forwarding messages. VantagePointe Financial Group sensitive information must not be forwarded to any party outside VantagePointe Financial Group without the prior approval of a manager. Blanket forwarding of messages to parties outside VantagePointe Financial Group is prohibited unless the prior permission has been obtained. Messages sent by outside parties should also not be forwarded to other third parties unless the sender clearly intended this and unless such forwarding is necessary to accomplish an ordinary business objective.

A5. Access Policy for VantagePointe Financial Group Contractors

Objective

The objective of this document is to provide a security policy to be followed by the support contractors of VantagePointe Financial Group Management (henceforth referred to as VantagePointe Financial Group).

Scope

The scope of this document is to establish a "baseline" or a "standard of due care" to which all parties to the arrangement must abide. This baseline must define the minimum cybersecurity requirements that must be maintained in order to participate in the networking arrangement.

Access Guidelines

- All user-ids created in the Partner Access environment will be assigned to specific users. Generic accounts shall not be created and requests for the same will not be encouraged.
- All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "pseudo" must have a unique password from all other accounts held by that user.
- Passwords shall not be inserted into e-mail messages or other forms of electronic communications.
- All user-level and system-level passwords must conform to the Password Guidelines described below.
- Password must be changed on new accounts at first login within one business day of receiving the account setup information.
- User privileges for offsite contractors are assigned on a need-to-access basis with the consent of the VantagePointe Financial Group IT organization. Any attempt to bypass security measures put in place by the VantagePointe Financial Group IT organization will be considered a breach of VantagePointe Financial Group security policies and appropriate action may be taken including all termination of VantagePointe Financial Group network access for such individuals.
- Any attempt to share passwords or to use credentials not explicitly assigned to that user will also constitute a breach of VantagePointe Financial Group security policies.
- If a VantagePointe Financial Group contractors from a contracted VantagePointe Financial Group leaves that VantagePointe Financial Group or the VantagePointe Financial Group project for any reason, that VantagePointe Financial Group shall notify VantagePointe Financial Group of the departure within one business day of the contractors' departure.
- In addition, VantagePointe Financial Group reserves the rights to revoke privileges on dormant user-Ids automatically. Dormant user-ids are those which have not been used to login for a period of more than 30 days.
- VantagePointe Financial Group authentication systems will enforce automatic session time-out after no activity for a designated period. On secured tokens, this period will be set to sixty minutes.

- All offsite contractors will be required to authenticate to a firewall prior to receiving any access to VantagePointe Financial Group resources. Such access shall be granted only for the duration of the authenticated session.

Password Guidelines

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, VantagePointe Financial Group, admin etc.
    - Strong passwords have the following characteristics:
    - Contain both upper and lower case characters (e.g., a-z, A-Z)
    - Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
    - They are at least eight alphanumeric characters.
    - They are not a word in any language, slang, dialect, jargon or based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least seven alphanumeric characters.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

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

Encryption and Authentication Considerations

Encryption processes shall be employed for sensitive transmitted data transmitted over the Internet.
All connections to VantagePointe Financial Group systems will be done with secure protocols such as SSH where possible.

Change Control and Contingency Planning Considerations

- Virus detection and eradication software and procedures will need to be in place for any and all systems which access the VantagePointe Financial Group network or related resources in any way.

- All modifications to networks accessing VantagePointe Financial Group network will need to go through an appropriate change control and approval process, which includes but is not limited to notifying VantagePointe Financial Group IT.

- Contracted VantagePointe Financial Group networks, which connect to the VantagePointe Financial Group networks in any way will complete rapid installation of patches from firewall & operating system vendors in the event of vulnerabilities being made public.

- The network and security administrators for contracted companies shall notify VantagePointe Financial Group Network Operations of any breaches and compromises of their networks. This information will be strictly used by VantagePointe Financial Group to prevent and deter attacks to VantagePointe Financial Group resources. Such companies shall deploy and actively manage intrusion detection systems to notify Run228 about attempted or successful break-ins. Such a report will need to be submitted to the VantagePointe Financial Group Helpdesk within four hours of discovery.

- Onsite contractors at any VantagePointe Financial Group facilities shall register their non-VantagePointe Financial Group provided machines with the VantagePointe Financial Group Help Desk located at the local VantagePointe Financial Group facility so as to ensure compliance with VantagePointe Financial Group desktop policies and standards.

A6. Server Policy

Purpose

The objective of this policy is to provide information security instructions applicable to all server and network equipment.

Scope

All VantagePointe Financial Group IT personnel who manage and direct server and storage assets.

Introduction

VantagePointe Financial Group has outsourced its IT management to Run228. This policy seeks to maintain common guidelines in the operation and management of these production-critical servers, storage and network devices by Run228.

Guidelines

Business Use Only: VantagePointe Financial Group computer and communication systems must be used only for business purposes. Personal use, even incidental, is not permitted on any computer servers or networking gear. Examples of personal use include MP3 servers, game servers, and surfing the Internet for entertainment purposes.

Changes to Application Software: Run228 has a standard list of permissible hardware and software packages that can run in the corporate data center. Business owners must not install other software packages on any Operations maintained servers in the datacenter without obtaining advance permission from the DESIGNATED INDIVIDUAL. Auto-discovery license management software may be used to remotely determine which software packages are resident on user computer hard disks. Unapproved software may be removed.

Changes to Operating System Configurations: On supported computer hardware, business owners must not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they will be performed by Run228 staff after proper review.

Changes to Hardware: Computer equipment in the data center must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without the prior knowledge of and authorization from the DESIGNATED INDIVIDUAL. Auto-discovery software may be used to determine what equipment is installed in each server, so any unauthorized hardware reconfigurations are detected automatically.

Access Control Package: All VantagePointe Financial Group computers must run an access control packageapproved by the DESIGNATED INDIVIDUAL. Typically these packages require a fixed password at the time a computer is booted and again after a certain period of no activity. Users must set the time frame for this period of no activity -- at which point the contents of the screen are obscured -- to 15 minutes or less. If sensitive information resides on a computer, the screen must be protected with an access control package.

Choice and Storage of Passwords: The user-chosen passwords employed by access control software packages, should follow the guidelines specified in the Password Policy. Users must maintain exclusive control of their personal passwords; they must not share them with others at any time. Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access controls, or in any other locations where unauthorized persons might discover them.

Security and Hardening: All servers in the datacenter will undergo review by the DESIGNATED INDIVIDUAL for security and hardening. Externally available machines, slated for installation in the DMZ or other Internet connected networks will undergo a more thorough and strict hardening evaluation.

Logging Of Events Related To Secret Information: Servers in the datacenter must securely log all significant computer security and operation relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software. Examples of operational events include Operating system errors or warnings, which might need operator intervention. Entreda Unify maintains log data from servers in addition to local logging on the server in question. Logs should be kept for a minimum of one month and then archived.

Virus Program Installed: All Windows based servers, must continuously run the current version of the selected virus detection package approved by the DESIGNATED INDIVIDUAL. Business owners must not abort or uninstall the virus scan program, especially when they are connected in any way to the VantagePointe Financial Group internal network. Entreda Unify™ will check for and approved virus protection program and has the ability to auto remediate the situation by installing a virus checker on the device. (Window or Mac)

Decompression before Checking: Externally supplied media, and other removable storage media must not be used unless they have first been checked for viruses. Externally supplied computer-readable files (software programs, databases, word processing documents, spreadsheets, etc.) must be decompressed prior to being subjected to an approved virus checking process. If the files have been encrypted, they must be decrypted before running a virus-checking program. Sometimes, virus-checking programs cannot detect viruses in compressed or encrypted files.

Eradicating Viruses: Because viruses can be complex and sophisticated, business owners must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately stop using the involved computer, disconnect the computer from all networks, and contact the DESIGNATED INDIVIDUAL for help. If the suspected virus appears to be damaging information or software, users must immediately turn-off the infected computer.

Patches and Security Updates: If a vulnerability is discovered on any production critical server or network gear, emergency downtime must be scheduled and the vulnerability should be patched after appropriate analysis.

Periodic Back-Up: All sensitive, valuable, or critical information resident on VantagePointe Financial Group servers must be periodically backed-up. Such back-up processes should be performed daily, and at a minimum, weekly backups must be performed. Selected files from back-ups must be periodically restored to demonstrate the effectiveness of every back-up process.

Copyright Protection: VantagePointe Financial Group, strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Making unauthorized copies of licensed and copyrighted software, even if only for "evaluation" purposes, is strictly forbidden. Likewise, VantagePointe

Financial Group allows reproduction of copyrighted materials only to the extent legally considered "fair use" or with the permission of the author/owner. If users have any questions about the relevance of copyright laws, they should contact corporate legal counsel. Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.

Downloading Sensitive Information: Sensitive VantagePointe Financial Group information may be downloaded from a multi-user system to a desktop/laptop computer only after two conditions have been fulfilled. For this data transfer to take place, a clear business need must exist and advance permission from the information Owner must be obtained. This policy is not intended to cover e-mail or memos, but does apply to databases and other information stored on the company's servers.

Tools to Compromise Systems Security: Unless specifically authorized by the DESIGNATED INDIVIDUAL, VantagePointe Financial Group users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

A7. Firewall Policy

Purpose

This purpose of this policy is to standardize the management and maintenance of firewalls or filtering devices within the VantagePointe Financial Group's network.

Scope

This policy defines the essential rules regarding the management and maintenance of firewalls at VantagePointe Financial Group and it applies to all firewalls controlled by Run228.

Introduction

Firewalls are an essential component of VantagePointe Financial Group's information systems security infrastructure. Firewalls are defined as security systems that control and restrict both Internet/Extranet connectivity and Internet/Extranet services. Firewalls establish a perimeter where access controls are enforced. Connectivity, as the word is used here, defines which computer systems can exchange information. A service, as the word is used here, is sometimes called an application, and it refers to the way for information to flow through a firewall.

In some instances, systems such as routers or gateways may be functioning as though they are firewalls when in fact they are not formally known as firewalls. All VantagePointe Financial Group systems playing the role of firewalls, whether or not they are formally called firewalls, must be managed according to the rules defined in this policy. In some instances this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

Guidelines

Defined Decision Maker: Before being enabled, all new firewall services and new connectivity paths must be evaluated in terms of business advantages and security risks. The DESIGNATED INDIVIDUAL is the only recognized decision maker who can either approve or deny these requests.

Regular Auditing: Because firewalls provide such an important barrier to unauthorized access to VantagePointe Financial Group networks, they must be audited on a regular basis. At a minimum, this audit process must include consideration of defined configuration parameters, enabled services, permitted connectivity, current administrative practices, and adequacy of the deployed security measures. These audits must also include the regular execution of vulnerability identification software.

Logs: All changes to firewall configuration parameters, enabled services, and permitted connectivity must be logged. In addition, all suspicious activity, which might be an indication of unauthorized usage or an attempt to compromise security measures, must also be logged. These logs must be promptly removed from the recording systems and stored in a physically protected container for at least six months after the

time they were recorded. These logs must be reviewed periodically to ensure that the firewalls are operating in a secure manner.

Intrusion Detection: VantagePointe Financial Group firewalls should work in conjunction with intrusion detection systems approved by the Network Operations department. These intrusion detection systems must each be configured according to the specifications defined by the Network Operations department. All Network Operations staff working on firewalls must be provided with remote access systems and privileges so that they can immediately respond to these incidents even when they are physically removed from the firewall in question.

Disaster Recovery and Business Continuity Planning: VantagePointe Financial Group must have a contingency plans which address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, and Internet Service provider (ISP) unavailability. These contingency plans must be kept up-to-date to reflect changes in the systems environment. These plans must also be periodically tested to ensure that they will be effective in restoring a secure and reliable information systems environment.

External Connections: All in-bound real-time Internet connections to VantagePointe Financial Group internal networks and/or multi-user computer systems must pass through a firewall before users can reach a login banner. Aside from personal computers, which access the Internet on a single-user session-by-session dial-up basis, no VantagePointe Financial Group computer system may be attached to the Internet unless it is protected by a firewall. Wherever a firewall supports it, log-in screens must have a notice indicating that: (1) the system may only be accessed by authorized users, (2) users who log-in represent that they are authorized to do so, (3) unauthorized system usage or abuse is subject to disciplinary action including criminal prosecution, and (4) system usage will be monitored and logged.

Default to Denial: Every Internet connectivity path and Internet service not specifically permitted by this policy must be blocked. The list of currently approved services must be documented and distributed to all with a need-to-know. Likewise, every network connectivity path not specifically permitted by the Run228 team must be denied by firewalls. Permission to enable any paths will be granted by the Network Operations Department only when (1) the paths are necessary for important business reasons, and (2) sufficient security measures will be consistently employed.

Virtual Private Networks: To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic (with the exception of Internet mail and push broadcasts) accessing VantagePointe Financial Group networks must be encrypted with the products approved by the Network Operations Department. These connections are called virtual private networks or VPNs. Many VPNs combine extended user authentication functionality with encryption functionality.

Firewall Access Mechanisms: The firewall(s) must have unique passwords or other access control mechanisms. In other words, the same password or access control code must not be used on other types of systems.

Firewall Access Privileges: Privileges to modify the functionality, connectivity, and services supported by firewalls must be restricted to a small number of technically-trained individuals. These privileges must be granted only to individuals who are responsible for the maintenance and updating of the firewall(s). All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require. Care must be taken to schedule out-of-town vacations so that at least one of these firewall administration staff members is readily available at all times.

Network Management Systems: Firewalls must be configured so that they are visible to internal network management systems. Firewalls must also be configured to permit the use of remote automatic auditing tools to be used by authorized staff members. Unless deliberately intended as a test, such automatic auditing tools must not trigger a response sequence through firewall-connected intrusion detection systems.

Disclosure Of Internal Network Information: The internal system addresses, configurations, and related system design information for VantagePointe Financial Group networked computer systems must be restricted such that both systems and users outside VantagePointe Financial Group internal network cannot access this information. One example of this involves split DNS (Domain Name Service).

Firewall Dedicated Functionality: Firewalls must run on dedicated machines which perform no other services (such as acting as a mail server). To reduce the chances of security compromise, firewalls must have only the bare minimum of operating systems software resident and enabled on them

Firewall Change Control: Because they support critical VantagePointe Financial Group information systems activities, firewalls are considered to be production systems. This means that all changes to the software provided by vendors (excluding vendor-provided upgrades and patches) must be approved in advance by the Run228 before being used in a production environment.

Monitoring Vulnerabilities: The team members responsible for managing firewalls must subscribe to relevant sources providing current information about firewall vulnerabilities. Any vulnerability that appears to affect VantagePointe Financial Group networks and systems must promptly be brought to the attention of the Run228.

Standard Products: Unless advance written approval is obtained from the designated individual only those firewalls approved may be deployed with VantagePointe Financial Group networks. These firewalls will be installed, managed and maintained by the system administer.

Firewall Physical Security: Firewalls must be located in locked cabinet accessible only to those who must have physical access to such firewalls to perform the tasks assigned by management. The placement of firewalls in the open area within a general-purpose data processing center is prohibited, although placement within separately locked rooms or areas which are within a general data processing center is acceptable. Such firewalls must be placed on UPS power so that power interruptions do not affect the file systems on the firewalls.

Area	Response
Do you have any servers? If yes, how many?	**Yes** **4**
Is it an app server?	**No** **List all physical app servers:** **List all virtual app servers:**
Is it a web server?	**No** **List all physical web servers:** **List all virtual web servers:**
Is it a file server?	**No** **List all physical file servers:** **List all virtual file servers:**
How many routers do you have?	**5** **List of routers:**
How many firewalls do you have?	
How many ethernet switches do you have?	**List of ethernet switches:**
How many local desktops or laptops or servers do you use at your firm?	**100**
What is your preferred method of us accessing your network temporarily?	**None**