CYBER SECURITY POLICY

Document History and Distribution

Revision History

Revision #	Revision Date	Description of Change
1	11/26/18	Initial draft of document
2	12/09/19	Annual Review/Update
3	02/10/21	Annual Review/Update
4	06/21/22	Annual Review/Update

Distribution

Recipient	Distribution Method
Clarence Yee, President	Physical Delivery
Nicholas Cochran, Vice President	Physical Delivery
Emmanuel Comes, Compliance Officer	Physical Delivery
Laura Wich, Operations Manager	Physical Delivery
AIC Home Office Staff	Physical Delivery
AIC Registered Representatives	Electronic/Online

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 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 Cyber Security 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 Cyber Security 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 American Investors Company 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 American Investors Company 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 employees and contractors.
- Inventory of systems is included in Appendix B.

1.2 Security Policy Acknowledgement

All American Investors Company personnel will receive a copy of the Corporate Cyber Security Policy. Updates of the Cyber Security Policy will be posted online.

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.

2.2 Classification of Computer 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.

2.3 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 cyber security requires the active support and ongoing participation of executive staff, and all employees and management levels of the organization.

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 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

5. Limiting Private Information

American Investors Company 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. American Investors Company 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 American Investors Company managed facilities.

6.1 Locks and Barriers

American Investors Company operates in multiple office locations. Physical access to every office and work area containing sensitive American Investors Company information 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. 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 should be physically protected and encrypted to protect data against loss. The server room in the Home Office will be kept locked and the file room will be locked at the end of each business day.

Authorization from American Investors Company 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 should use encryption to protect sensitive information.)

6.2 Building Access Records

When a staff member terminates his/her relationship with American Investors Company, 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 may 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.
- 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 WatchGuard M200 Firewall. Not less frequently than once during each 12- month period, all operating systems shall be upgraded with any currently available security patches or other security-related enhancements available from the providers of such systems. The Entreda Unify platform is designed to correct non-compliance of the firewall and to alert the user 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.
- 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 should be verified on a periodic basis.

- American Investors Company 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.

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:

- Individuals responsible for hiring shall check the references and background of any prospective personnel who may have access to Private Information.
- Each individual who is hired by American Investors Company will be provided with a copy of the current Security Policy.
- American Investors Company conducts periodic training to remind individuals of existing polices and threats and to identify 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; avoiding the transmission of unencrypted Private Information on public networks; and disposing of Private Information in a secure manner.
- Employees are encouraged to report any suspicious or unauthorized use of Private Information to American Investors Company.

10. Breaches of Security

American Investors Company 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 AIC. All such events will be logged 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 periodically evaluated. Where possible and appropriate, security procedures may be tested and verified. 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. A sample report is attached in Appendix A.

12. Security Program Evaluation and Adjustment

American Investors Company will continually evaluate and adjust this Policy in light of the results of the monitoring of the overall information security program contemplated by this Policy. AIC 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.

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

13. Acknowledgment

The undersigned hereby acknowledges the terms and conditions of the American Investors Company Cybersecurity Policy.

Accepted by:

Clarence Yee, President

_____
(Signature)

_____
(Date)

Nicholas Cochran, Vice President

_____
(Signature)

_____
(Date)

Emmanuel Comes, Compliance Officer

_____
(Signature)

_____
(Date)

Laura Wich, Operations Manager

_____
(Signature)

_____
(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 – Device Inventory

SEE ATTACHED

All devices are classified as RED or GREEN. Because all GREEN systems have access to RED systems, they will be subject to the same restrictions as RED system users and will assume the highest security level.

Appendix C – 3rd Party Service Vendors

AppRiver
Corodata
Charles Schwab
Datto
Entreda
Global Relay
iland/Veeam
Iron Mountain
LastPass
Morningstar
National Financial Services, LLC / Fidelity
Novani, LLC
Sfax
SIGNiX
Splashtop
TD Ameritrade
Techmate/WinOPS

Appendix D - Policy Documents

D1 Personal Computer and BYOD Policy

Objective

The objective of this policy is to provide information security instructions applicable to all users who use American Investors Company Personal Devices.

Scope

All American Investors Company users are expected to comply with this policy. This policy applies whether computers/devices are stand-alone or connected to the American Investors Company network.

Introduction

A large portion of American Investors Company 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 American Investors Company.

American Investors Company conducts business in the Home Office with 13 desktops and 1 server. These devices are expected to have access to PII data. See Appendix B for list of devices.

Guidelines

Business Use Only: American Investors Company 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: American Investors Company has permissible software packages for Home Office PCs. Home Office users must not install other software packages on Business Use PCs without obtaining advance permission.

Changes to Operating System Configurations: On Home Office business use computer hardware, users must not change operating system configurations, upgrade existing operating systems, or install new operating systems without obtaining advance permission.

Access Control: All American Investors Company computers must run an access control package (ie: Screen Saver lockout). 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). American Investors Company 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: American Investors Company users may join their computers to the corporate domain. This enables all American Investors Company computers to be managed and protected. In this scenario, users are not permitted to change administrative privileges on any American Investors Company owned computers. IT System Administrators should have administrative access to all American Investors Company owned computers.

Laptop physical security: All American Investors Company 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 American Investors Company approved virus detection package. Users must not abort or uninstall the virus scan program, especially when they are connected in any way to the American Investors Company sensitive data. American Investors Company 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. 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 American Investors Company computer system. (Viruses, worms, or a Trojan horses.)

Periodic Back-Up: All sensitive, valuable, or critical information resident on American Investors Company computer systems must be periodically backed-up. Such back-up processes must be performed at least weekly. American Investors Company Home Office utilizes Veeam to perform local backups and iland/Veeam for offsite backups.

Copyright Protection: American Investors Company, 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, American Investors Company allows reproduction of copyrighted materials only to the extent legally considered "fair use" or with the permission of the author/owner. Unless they receive information to the contrary, users should assume that software and other materials are copyrighted.

Downloading Sensitive Information: Sensitive American Investors Company 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 American Investors Company 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, users must not acquire, possess, trade, or use hardware or software tools that could be employed to 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.

Reporting Problems: Users must promptly report information security alerts, warnings and suspected vulnerabilities.

D2 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 American Investors Company facility, has access to the American Investors Company network, or stores any non-public American Investors Company 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 American Investors Company entire corporate network. As such, all American Investors Company employees (including contractors and vendors with access to American Investors Company systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

General

- All user-level passwords for systems containing PII should be changed at least every six months.
- 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 passwords 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 American Investors Company accounts as for other non-American Investors Company access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various American Investors Company 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 American Investors Company passwords with anyone
- All passwords are to be treated as sensitive, Confidential American Investors Company information.
- Here is a list of "DON'Ts":
    - Don't reveal a password over the phone
    - 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.
    - Change passwords at least once every six months (except system-level passwords which must be changed quarterly).
- If a senior staff member leaves the American Investors Company for any reason, all administrator passwords will be immediately changed.
- AIC personnel must enable auto locking password-protected screensavers on their desktops/laptops to prevent misuse if they are absent from their desks.

D3 Acceptable Use and Internet Policy

Objective

The objective of this policy is to provide cyber security instructions applicable to all users (employees, contractors, consultants, temporaries, vendors, etc.) who use American Investors Company Internet Resources.

Scope

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

Introduction

American Investors Company provides the use of the Internet as a productivity enhancement tool. American Investors Company 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 American Investors Company 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-American Investors Company sources via the Internet must be screened with virus detection software prior to being used in any way. Refer to American Investors Company 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 American Investors Company 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 American Investors Company business, or make modifications to existing web pages dealing with American Investors Company business unless they have first obtained approval from the Compliance Department. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page.

Information Confidentiality

Information Exchange: All American Investors Company software, documentation and other internal information must not be sold or otherwise transferred to any non- American Investors Company party for any purposes other than business purposes expressly authorized by management.

Posting Materials: Users must not post unencrypted American Investors Company material (software, internal memos, policies, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar publicly accessible services, unless the Compliance Department has first approved the posting of these materials. In more general terms, American Investors Company 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, American Investors Company 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.

Intellectual Property Rights

Copyrights: American Investors Company strongly supports strict adherence to software vendors' license agreements. When at work, or when American Investors Company 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 American Investors Company internal computers via the Internet must authenticate themselves before gaining access to American Investors Company internal network

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, American Investors Company computer users must refuse all offers by software to place a cookie on their computer for websites containing PII so that they can automatically login the next time that they visit a particular Internet site.

Establishing Network Connections: Unless prior approval has been obtained, users may not establish Internet or other external network connections that could allow non-American Investors Company users to gain access to American Investors Company 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 American Investors Company resources is strictly prohibited. Any such activity will be treated as a malicious attack on American Investors Company computing resources.

Personal Use

Personal Use: American Investors Company 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 American Investors Company and is strictly prohibited. Use of P2P is against policy. American Investors Company utilizes Entreda Unify to monitor if P2P software installed on any PCs, MACs and mobile devices.

Blocking Sites: American Investors Company firewalls may prevent users from connecting with certain non-business web sites. American Investors Company 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 American Investors Company systems are permitted to visit that site. Users shall not use non-American Investors Company resources for the purposes of testing and other business-related purposes without the permission of the owners of such resources.

Privacy

No Default Protection: American Investors Company 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, American Investors Company 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 American

Investors Company computers. Such management access assures compliance with internal policies, assists with internal investigations, and assists with the management of American Investors Company information systems.

Logging: American Investors Company may routinely log web sites visited, files downloaded and related information.

Junk E-mail: Users are prohibited from using American Investors Company 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 American Investors Company 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: AIC 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 American Investors Company 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. 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 must not personally redistribute system vulnerability information or post it on any public forum.

Testing Controls: Users must not "test the doors" (probe) security mechanisms at either American Investors Company or other internet sites.

D4 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 American Investors Company-owned and maintained mail system.

Introduction

American Investors Company IT provides the use of e-mail as a productivity enhancement tool; American Investors Company 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 American Investors Company.

Guidelines

Authorized Usage: American Investors Company 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 American Investors Company 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 American Investors Company 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 American Investors Company comes to an end, all the user's privileges on American Investors Company 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.

User Accountability: Regardless of the circumstances, individual passwords should not be shared or revealed to anyone.

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.

Use Only American Investors Company E-Mail Systems: Unless approved by American Investors Company, users must not use their personal e-mail accounts with an Internet Service Provider (ISP) or any other third party for any American Investors Company business messages. To do so would circumvent logging, SPAM control, virus prevention and backup controls that American Investors Company has established. 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 American Investors Company 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 American Investors Company information on the Internet only if the information has been officially approved by American Investors Company for public release.

No Guaranteed Message Privacy: American Investors Company 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 American Investors Company. As a matter of standard business practice, all American Investors Company electronic mail communications must be consistent with conventional standards of ethical and polite conduct.

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

Harassing or Offensive Materials: American Investors Company 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 American Investors Company 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 American Investors Company in order to assist with the investigation of a complaint).

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

Public Representations: No media advertisement, Internet home page, electronic bulletin board posting or any other public representation about American Investors Company may be issued unless it has first been approved by the Compliance Department.

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. American Investors Company sensitive information must not be forwarded to any party outside American Investors Company without the prior approval of a manager. Blanket forwarding of messages to parties outside American Investors Company 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.

D5 Firewall Policy

Purpose

This purpose of this policy is to standardize the management and maintenance of firewalls or filtering devices within the American Investors Company*'s* network.

Scope

This policy defines the essential rules regarding the management and maintenance of firewalls at American Investors Company.

Introduction

Firewalls are an essential component of American Investors Company'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.

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 American Investors Company 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.

Logs: Changes to firewall configuration parameters, enabled services, and permitted connectivity should be documented. In addition, all suspicious activity, which might be an indication of unauthorized usage or an attempt to compromise security measures, should be logged.

External Connections: All in-bound real-time Internet connections to American Investors Company 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 American Investors Company computer system may be attached to the Internet unless it is protected by a firewall.

Default to Denial: Every Internet connectivity path and Internet service not specifically permitted by this policy may be blocked.

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.

Disclosure Of Internal Network Information: The internal system addresses, configurations, and related system design information for American Investors Company networked computer systems must be restricted such that both systems and users outside American Investors Company 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 American Investors Company 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 before being used in a production environment.

Firewall Physical Security: Firewalls should be located in a secure area. Such firewalls should be placed on UPS power so that power interruptions do not affect the file systems on the firewalls.