Independent Wealth Network

2350 NW 128th Street
Urbandale, Iowa 50323
515-461-5123

www.indwealth.net

Cyber Security Policies

Effective January 6, 2025

Independent Wealth Network

Cyber Security Policies

Table of Contents

Statement of General Policy

The general policy of Independent Wealth Network, Inc. ("IWN" or "firm") is to recognize the general increase in cyber security threats and develop processes necessary to ensure reasonable security of client information that is maintained electronically. It is not our intention to impose restrictions contrary to our established culture of openness, trust, and integrity. We are committed to protecting IWN's personnel, associates, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Achieving effective security is a team effort involving the participation and support of every person associated with the firm who has access to information and/or information systems. These policies apply to employees, representatives of IWN and their staff, consultants, and other workers at IWN, including all personnel associated with third parties (all together "associated persons" or individually "associated person"). It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

These policies apply to the use of information, computers and devices, and network resources to conduct firm business or interact with business systems, both internal and external, whether owned or leased by the firm, persons associated with the firm, or a third party.

Everyone associated with IWN is responsible for exercising good judgement regarding appropriate use of information, devices, and network resources in accordance with firm policies and standards, legal standards, and regulations.

Acceptable Use Policy

The purpose of this policy is to outline the acceptable use of computer equipment at IWN. These rules are in place to protect client information, persons associated with the company, and the company itself. Inappropriate use exposes the firm to risks, including virus attacks, compromise of network systems and services, and potential legal issues.

General Use and Ownership

IWN information stored electronically, whether owned or leased by the firm, persons associated with the firm, or a third party remains the firm's sole property. You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of the firm's information. You may access, use, or

share the firm's information only to the extent it is authorized and necessary to fulfill your assigned job duties.

Security Requirements

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

All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended. Root encrption, virus & threat protection, and a software firewall must be activated on all devices which store client information.

Everyone is expected to use extreme caution before opening email attachments from unknown senders which may contain malware. Such emails should be considered "dangerous" and caution should be exercised before forwarding suspicious emails to other users without their advance knowledge.

Unacceptable Use

The activities listed below are, in general, prohibited. Exemptions may be granted from these restrictions for fulfillment of authorized legitimate job responsibilities (e.g., systems administrators may need to disable network access of a host if that host is disrupting other services). The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

Under no circumstances is an associated person authorized to engage in activity that is illegal under local, state, federal, or international law while using IWN resources.

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

The following system & network activities are strictly prohibited:

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

2. Unauthorized copying of copyrighted material including digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the firm or the end-user does not have an active license.
3. Accessing data, a server, or an account for any purpose other than conducting firm-related business, even if you have authorized access.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal. Management should be consulted prior to the export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.)
6. Revealing your password to others or allowing the use of your account by others. This includes family or other household members when work is being done at home.
7. Using an IWN computing asset to actively engage in procuring or transmitting material in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any IWN account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communications. Security breaches include, but are not limited to, accessing data of which the associated person is not expressly authorized to access unless these duties are within the scope of regular duties. For the purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior authorization from the Chief Compliance Officer ("CCO") is obtained.
12. Executing any form of network monitoring, which will intercept data not intended for the associated person's host, unless this activity is part of their normal job duties.
13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on any IWN network or system.
15. Interfering with or denying service to any user other than the associates host (for example, denial of service attack).

16. Using any program, script, command, or sending messages of any kind with the intent to interfere with or disable a user's terminal session, via any means, locally or remotely.
17. Providing information about, or lists of, associated persons to parties outside the firm without first obtaining consent from the CCO.

The following email and communication activities are strictly prohibited:

1. Sending unsolicited email messages, including "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, or messaging regardless of language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or collect replies.
5. Creating or forwarding "chain letters", Ponzi, or other pyramid schemes of any type.
6. Use of unsolicited email originating from within the firm's networks or providers on behalf of, or to advertise, any service hosted by the firm or connected via the firm's network.
7. Posting the same or similar non-business-related messages to larger numbers of news groups or message boards.

Social Media

Social Media use by associated persons, whether using the firm's property and systems or personal computing systems, is also subject to the terms and restrictions set forth in this policy. Limited and occassional use of IWN's systems to engage in social media use is acceptable, provided that it is done professionally and responsibly, complies with any applicable rules regarding advertising and correspondence, does not otherwise violate this policy, is not detrimental to the firm's best interests, and does not interfere with regular work duties. Social media use is subject to monitoring.

The Confidential Information Policy described in this policy also applies to social media use. As such, associated persons are prohibited from revealing any of the firm's confidential or proprietary information, trade secrets, or any other material covered by the Confidential Information Policy when engaged in social media use.

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

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Clean Desk Policy

A clean desk policy can be an important tool to ensure that all sensitive and confidential materials are removed from an end-user's workspace and locked away when the items are not in use or when the associated person leaves their workstation. It is one of the most effective strategies when trying to reduce the risk of security breaches in the workplace. This policy can also increase awareness of protecting sensitive information.

The purpose of this policy is to establish the minimum requirements for maintaining a "clean desk". This policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

This policy applies to all IWN associated persons.

- Computers must be locked when the workspace is unoccupied.
- Computers must be shut down completely at the end of the work day.
- Restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied or at the end of the work day.
- File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or unattended.
- Keys used for access to restricted or sensitive information must not be left at an unattended desk.
- Laptops must be secured with a locking cable or locked in drawer when not in use.
- Passwords may not be left on sticky notes posted on or under a computer. Nor may they be left written down in an accessible location.
- Printouts containing restricted or sensitive information should be immediately removed from the printer.
- For disposal, restricted or sensitive documents should be shredded or placed in locked official shredder bins.
- Whiteboards containing restricted or sensitive information should be erased.

- Treat mass storage devices such as USB drives as sensitive devices which should be secured in a locked drawer and encrypted.

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, periodic walk throughs, internal audits, and external audits. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Wireless Network Requirements

IWN recognizes that associated persons may use a variety of computer devices, networks, and other information systems in the execution of their normal job duties. Many of these devices have the capability of connecting wirelessly to networks. This section specifies the conditions to which wireless infrastructures must comply to avoid a potential security breach. This applies to all associated persons using any device capable of transmitting packet data.

General Requirements

All wireless infrastructure devices that connect to a network or provide access to confidential, restricted, or sensitive information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.
- Bluetooth devices must use Secure Simple Pairing with encryption enabled.

Home or Remote Wireless Device Requirements

All home or remote wireless infrastructure devices that provide access to IWN systems, networks, or information must:

- Enable Wi-Fi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS.

- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point.
- Disable broadcast of SSD.
- Change the default SSID name.
- Change the default login and password.

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Remote Access Policy

Remote access to IWN systems and information is essential to maintain productivity, but in many cases this access may originate from networks that may already be compromised or have a significantly lower security posture than our firm's requirements. While these networks are beyond our control, we must mitigate these external risks to the best of our ability.

This section refers to remote access used to do work on behalf of IWN, including reading or sending email and accessing web-based systems, by any associated person. Failure to comply with these requirements exposes the firm to loss of sensitive or confidential information, damage to public image, fines, or other financial liabilities.

Remote access must be via a compliant secure encrypted system with a strong passphrase, or controlled with encryption via a Virtual Private Network (VPN).

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, inspections, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Passwords

Passwords are a critical component of information security serving to protect user accounts. However, poorly constructed passwords may compromise systems or data. The section applies to all associated persons to provide best practices for creating strong, secure passwords for user-level accounts, system-level accounts, web-based accounts, email accounts, screen saver protection, voicemail systems, and local router systems.

Password Construction Guidelines

All passwords must meet or exceed the following guidelines:

- Contain at least 12 characters.
- Contain both upper-case and lower-case letters.
- Contain at least one digit.
- Contain at least one special character (may vary based on specific system requirements, but examples include, $ % ^ & ( ) _ + | ~ - = \ ‘ { } [ ] : ” ; < > ? , /).

Poor or weak passwords have the following characteristics:

- Contain less than 8 characters
- Can be found in a dictionary, including foreign language, or exist in slang, dialect, or jargon.
- Contain personal information usch as birthdates, addresses, phone numbers, or names of family members, pets, friends, or fictional characters.
- Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Contain patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Contain common words spelled backwards, or preceeded or followed by a number (for example, terces, secret1, or 1secret).
- Are some version of “Welcome123”, “Password123”, or “Changeme123”.

You should never write down a password. Instead, try to create a password you can remember easily. One way to do this is to create a password based on a song title, an affirmation, or another phrase. For example, the phrase “This may be one way to remember: could become the password TmB1w2R! or another variation. (Note: Do not use these examples as passwords!)

Passphrases

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

A passphrase is similar to a password in use, however it is relatively long and constructed of multiple words which provides greater security against random, dictionary based, attempts to defeat the passphrase. Strong passphrases should follow the general password construction guidelines including upper- and lower-case letters, numbers, and special characters (for example, TheRoad2SuccessIs@lwaysUnderConstr!)

Password Protection Policy

- Users must not use the same password for firm-related accounts as for personal accounts.
- Where possible, users must not use the same password for multiple IWN systems.
- User accounts with system-level privileges granted through group memberships must have a unique password for all other accounts held by that user to access system-level privileges.
- All system-level passwords must be changed at least quarterly.
- All user-level passwords must be changed at least every six months. The recommended change interval is every four months.
- Passwords may not be shared with anyone, including assistants, managers, co-workers while on vacation, or family members. All passwords are to be treated as sensitive, confidential information.
- Other than temporary passwords which must be changed upon first use, passwords may not be inserted into emails or other forms of electronic communication.
- Other than temporary passwords which must be changed upon first use, passwords may not be revealed over the phone.
- Passwords may not be revealed on questionnaires or security forms.
- Do not hint at a password format (for example, "my family name").
- Do not write down or store passwords in your office. Do not store passwords in a file on a computer system or mobile device without encryption.
- It is acceptable to use certain encrypted password manager software packages which are publicly available. The CCO or delegate may approve a provider if requested.
- Do not use the "Remember Password" feature of applications or web browsers.
- Any user suspecting that their password has been compromised must immediately report the incident and change all passwords.
- Password guessing or cracking tools may be performed on a periodic or random basis by IWN. If a password is guessed or cracked during one of these scans, the user will be required to change it to comply with the Password Construction Guidelines.

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including but not limited to business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Digital Signature Policy

This section provides guidance on the use and acceptance of digital signatures as a substitute for "wet" signatures on forms, documents, and agreements. IWN must abide by the systems and policies employed by the variety of vendors and organizations the firm conducts business with. In general, if a digital signature fulfills the requirements of an approved custodian, IWN also accepts the digital signature. However, if the CCO determines that a particular custodian does not have sufficient security protocols in place to validate the identity of the signer, IWN may impose additional requirements.

IWN stand-alone documents may be signed digitally via DocuSign, but only when Knowledge-Based or SMS identity verification is used. IWN will also accept digitally scanned documents which were signed by traditional "wet" signature.

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Confidentiality Policy

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

- As necessary to provide the service the client has requested or authorized, or to maintain and service the client's account;

- As required by regulatory authorities or law enforcement officials who have jurisdiction over the firm, or as otherwise required by any applicable law; and
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

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

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Data Backup Policy

The purpose of this policy is to establish that all of IWN's data is backed up and recoverable in the event of a data breach or disaster. This policy applies to all systems, all data, and all associated persons.

All IWN data is stored on approved cloud-based systems purchased from third-party vendors. As part of IWN's annual vendor due-diligence, the CCO or designee is responsible for auditing each vendor for history of data breaches, security protocols, and to ensure the redundancy of data backup in multiple locations.

Associated persons are strongly discouraged from making backup copies of client data on devices not under direct control of IWN. If an associated person does make a backup copy, they are individually and solely responsible for safekeeping of that backup copy and agree to the following conditions:

- The data will be encrypted and password protected.
- In the event the device on which the data is stored becomes lost, stolen, or otherwise compromised, the associated person will immediately report the data loss to the CCO.

- The associated person agrees to reimburse IWN for all expenses and liabilities associated with the loss of data including, but not limited to, external consultants to evaluate and access the compromised data, the costs associated with recovering the data physically as well as the personnel resources dedicated to that task, the costs associated with notifying clients of the data breach, and the cost associated with protecting the client in the form of credit monitoring or other remedies which will be selected on effectiveness, not cost efficiency.

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Data Assessment & Breach Response Policy

IWN is committed to protecting our clients, associated persons, partners, and the firm itself from illegal or damaging actions by individuals either intentional or unintentional. We have a published Data Assessment & Breach Response Policy to define a breach, identify staff roles and responsibilities, and establish standards and metrics for reporting, remediation, and feedback mechanisms. Our intention is to focus significant attention on data security and how the firm should respond to a data security breach.

Any individual who suspects that a theft, breach, or exposure of IWN confidential information has occurred must immediately report their suspicion to the CCO and provide information about the reported issue. The CCO will investigate to determine if a theft, breach, or exposure has occurred and, if it has, activate the Breach Response plan below.

Breach Response Plan

IWN's response to a data breach will depend on the CCO's assessment of the type and severity of the incident. The CCO must analyze the breach in an attempt to determine the root cause, how the incident occurred, the types of data involved, the number of internal/external individuals and/or organizations impacted. The CCO is directed to:

- Contain and mitigate the incident/breach to prevent further damage.
- Evaluate the incident and assess the potential impact.
- Implement a disaster recovery plan, if needed.

- Alert the proper authorities (regulator(s), local law enforcement, FBI, United States Secret Service).
- Determine if the personal information of clients was compromised and notify affected clients within 30 days of the date the firm became aware of the breach.
- Enhance systems and procedures to prevent the recurrence of similar breaches.
- Evaluate the effectiveness of the response and update the response plan to address any shortcomings.

Periodic Assessment

At least annually, IWN will conduct an assessment to determine or detect potential systems vulnerabilities and ensure that cyber security procedures and processes effectively protect confidential information. Timely corrective action must be applied to any deficiencies detected.

Responsibility

The CCO or delegate will verify compliance with this policy through a variety of methods, including, but not limited to, business tool usage reports, internal and external audits, and systems monitoring. Any exception to the policy must be approved by the CCO or delegate in advance. Any associated person found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or association.

Approval

This Cyber Security Policy manual has been approved by Andrew Endelman, President & Chief Compliance Officer of Independent Wealth Network, Inc. on January 6, 2025.