Information Security Program Manual

December 2025

Table of Contents

Information Security Program/ Regulation S-ID

Name of Supervisor ("designated Principal"):	LFF, LFCM and LFAS AMLCO
Frequency of Review:	In daily course of business
How Conducted:	Customer file reviews Enforce information security procedures; train personnel in information protection
How Documented:	Account information Records of monitoring and testing, if required, of internal systems; ensure and document third party monitoring/testing of systems, if applicable.
WSP Checklist:	SEC Regulation S-ID
Comments:	Also reference Business Continuity Plan for technical details on document back-up and the Firm's Cybersecurity and ID Theft Prevention Program, if applicable.

Level Four Financial, LLC., Level Four Advisory Services, LLC., and Level Four Capital Management, LLC. (Collectively "the Firms") have adopted the following procedures in addition to those contained within its Cybersecurity and Identity Theft Prevention procedures to comply with Reg. S-ID and related state regulations regarding the protection of confidential client information and the reporting of breaches.

The Firms are committed to protecting the confidentiality of all nonpublic information regarding its clients and Associated Persons ("Nonpublic Personal Information").

It is each of the Firm's policy to protect, and maintain the accuracy of client personal information. To protect client personal information, the Firms have developed this Written Information Security Program ("WISP"). The intent of this WISP is to safeguard the Firm's storage of, access to, and disposal of client personal information, obtained and/or maintained in hard copy and/or electronically, as well as access and protection of its computer and information systems.

1.1 Nonpublic personal information ("NPI")

is defined as: personally identifiable information ("PII"). PII includes any information: a consumer provides to you to obtain a financial product or service from you about a consumer resulting from any transaction involving a financial product or service between you and a consumer; or you otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

1.2 Personal identifiable information ("PII")

is defined as: an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records is defined as: any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider is defined as: any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to clients

1.3 Safeguarding Customer Records and Information

The Firm and its employees are required to attempt to:

- Insure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

1.4 Storage and Access of Records on the Business Premises

1.4.1 Hard Copy/Paper Records

1. The Firm's offices are locked when the business is closed; unauthorized access is prohibited;
2. Records containing NPI shall be kept in a secure location such as an office or file room and/or locked file cabinet(s) unless the records are being currently used;
3. Access to records containing NPI shall be limited to those Associated Persons whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose;
4. Records should not be left on an Associated Person's desk when the Associated Person is not present unless the office space is secured;
5. Associated Persons will exercise due caution when mailing or faxing documents containing NPI or the Firm's proprietary information to ensure that the documents are sent to the intended recipients;
6. Associated Persons may only remove documents containing NPI or the Firm's proprietary information from Firm's premises for legitimate business purposes. Any documents taken off premises must be handled with appropriate care and returned as soon as practicable; and
7. Destruction of hard-copy confidential customer information is accomplished via a paper shredder or an outsourced secure document removal service approved by the Firm.

1.4.2 Disciplinary Measures for Violations

A copy of the WISP is to be distributed to each current Associated Person and to each new Associated Person on the beginning date of their employment. It shall be the Associated Person's responsibility for acknowledging in writing that he/she has received a copy of the WISP and will abide by its provisions. Associated Persons are encouraged and invited to advise the Designated Principal of any activities or operations which appear to pose risks to the security of personal information. If the Designated Principal is involved with these risks, Associated Persons are required to advise any other manager or supervisor or business owner.

In the event that an Associated Person is found to have violated the WISP, the Associated Person will be subject to disciplinary actions including, but not limited to: warnings; reprimands; suspension, termination, and/or referral to regulatory agencies. The nature and scope of the disciplinary action will be determined by the severity of the violation.

Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.

1.4.3 Terminated Employees

The Designated Principal will promptly disable system access for any terminated Associated Person. Terminated employees must return records containing personal data, in their possession at the time of termination as defined by the Firm's Privacy Policy. This includes all data stored on any portable device and any device owned directly by the terminated employee as applicable. In accordance with the Firm's privacy policy, FAs who leave the employment of the Firm may take certain customer contact information and NPI such as investment preferences if customers have not opted out of this information sharing. The Designated Principal will review customer choices in situations like these to prohibit unauthorized sharing.

A terminated employee's physical and electronic access to records containing NPI shall be restricted at the time of termination. This shall include deactivation of passwords/user IDs for remote electronic access to personal records, voice mail, internet, and email access. All Firm office keys, key cards, access devices, badges, Firm IDs, business cards, and the like shall be surrendered at the time of termination.

1.4.4 Working in Public Places

Associated Persons should avoid discussing NPI and the Firm's proprietary information in public places where they may be overheard, such as in restaurants and elevators. Associated Persons should be cautious when using laptops or reviewing documents that contain NPI and the Firm's proprietary information in public places to prevent unauthorized people from viewing the information.

1.4.5 Access to the Firm's Premises

The Firm's premises shall be secure from unauthorized access. The Designated Principal will conduct due diligence of registered locations for privacy policies and procedures as well as un-related third-party access to the location. No un-related third parties may conduct business at the same address/space without CCO approval

Meetings with clients should be held in conference rooms or other locations where NPI is not available or audible to others.

Visitors will be supervised while in the Firm's office.

1.5 Cybersecurity Program

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. For a number of years, Firms have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to financial institutions associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents. In general, cyber incidents can result from deliberate attacks or unintentional events. The industry has observed an increased level of attention focused on cyber-attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber-attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber-attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.

Protection of financial and personal customer information is a key responsibility and obligation of our Firm. Our Firm is required to have procedures in place to protect against any anticipated threats or hazards to the security or integrity of customer records and Nonpublic Personal Information and against unauthorized access to or use of customer records or information. We realize that customer information and records can be compromised in a variety of ways.

As a Broker-Dealer, we are required to address the potential risks of brokerage accounts or transaction intrusions whereby an unauthorized person gains access to a customer account, transaction, or monies and either steals available assets or misuses the account to manipulate the market. Intrusions are generally accomplished through the theft of the login credentials of a customer or Firm employee.

1.5.1 Access to and Security of Electronic Records

The Firms have implemented the following cybersecurity procedures to protect Nonpublic Personal Information and the Firm's proprietary information. This policy shall apply to all electronic devices (i.e. computers, laptops, tablets, smartphones, and other similar devices), whether Firm owned or employee owned, which are used to conduct Firm business (hereafter "Electronic Devices"):

1. The Firms requires relatively "strong" passwords, such as combinations of lower case letters, upper case letters, and numbers or symbols to protect Electronic Devices and systems utilized on such devices. Associated Persons must never share their passwords or store passwords in a place that is accessible to others and should refrain from using passwords that would be easily guessed, such as children's names, birthdays, or commonly used strings like "password" or "12345".
2. Associated Persons should shut down or lock their computers when they leave the Electronic Devices for any extended period of time;
3. Associated Persons should change passwords periodically and not use the same password across multiple platforms. If a password is compromised, the Associated Person must change his or her password immediately and promptly notify the Designated Principal of the breach;
4. Any theft or loss of an Electronic Device must immediately be reported to the Designated Principal;
5. All laptops and portable storage devices containing Nonpublic Personal Information should be encrypted;
6. Associated Persons should not click on unknown links in email or on the internet. When sending email with sensitive data, Associated Persons must type "Secure" in the subject line to encrypt the message.
7. Associated Persons are responsible for implementing and maintaining appropriate protections for Electronic Devices and the systems utilized on such devices, including:
    i. Anti-virus software,
    ii. Firewalls,
    iii. Prompt implementation of system patches and updates,
    iv. Encryption of all wireless data transmissions of sensitive data.
8. When technically feasible, Associated Persons access permissions should be restricted to those resources necessary for each Associated Person's business functions.
9. Secure connections shall be established, such as through a "VPN", when accessing the Firm's network remotely.
10. Terminated employee access permissions to the Clearing Firm and email shall be promptly disabled.
11. Information may be retained on conventional media, such as laptops and compact discs, as well as electronic equipment such as fax machines and photocopiers. Prior to sale or disposal, such devices will be permanently erased or destroyed.

1.5.2 Client Online Account Access

Many cybersecurity experts have identified account takeovers as the top risk. The Firms restrict client online account access at the clearing firm to view only. Client online account permissions are established by client request and does not facilitate transactions.

1.5.3 Access to Firm Networks

The Firms restrict access to network resources to Home Office associates to the extent necessary to accomplish their business functions. Branch associates and clients do not have access to the Firm's network.

1.5.4 Annual Information Technology Review & Risk Assessment

A cybersecurity risk assessment is a process where we are required to identify and analyze potential dangers or risks to our Firm's business that could arise from our information technology systems. Our Firm performs an annual risk and technology review in which we identify risks associated with our Firm's assets and vendors, and potential dangers or risks to our Firm that may arise through our information technology systems. These risks could include the compromise of customer or Firm confidential information, the misuse of customer funds or securities resulting in potential financial losses for our Firm or our clients, the theft of proprietary systems, or negative reputational impacts to the Firm. As part of our risk assessment process, below are areas that will be reviewed.

1.5.4.1 Assessing Threats and Vulnerabilities

When assessing threats or vulnerabilities the Firms will consider past cybersecurity incidents either at our Firm or noted within the industry, along with threat intelligence identified from other organizations or through security organizations. These threats or vulnerabilities may be internal (threats from Associated Persons), or external (threats from hackers or crime groups). If any threats or vulnerabilities are determined, the Firm will assess each threat or vulnerability based on risk and determine an appropriate means to address the issue.

1.5.4.2 Identification of Risks/Cybersecurity Governance

The Firm's will conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences and will document the date on which the risk assessment took place.

1.5.4.3 Defining Asset Inventories and Reviewing Critical Assets

Our Firm may use a variety of criteria to define what assets we have, what assets are authorized to be on our network, what assets are most important to protect, and identify our critical assets. Identifying critical assets is part of our obligation under Regulation S-P to protect customers' identifiable information. Therefore, databases containing personal information on our customers and business applications that use this information would be considered a critical asset. Other areas that may be identified as critical assets include, but are not limited to:

- Information contained in trading systems;
- Whether clients have online access to initiate transactions
- If there is an impact to order routing such as order management systems,
- Whether client statements data can be altered; and
- Whether a client's delivery of cash or securities would be compromised.

The Firm will perform a review of its critical information technology which includes hardware, software, programs, firewalls, etc., to identify any potential risks and implement such preventive, detective, corrective, or predictive controls. The review will be done either internally or the Firm may hire a third party to perform a risk assessment of the Firm's IT program. The review will be documented in a written report or other hard copy format and given to the AMLCO and Information Security Committee for review.

1.5.5 Vendor Management

Across the industry, it is common practice for Firms to rely on third party vendors for a range of services. However, outsourcing to third party vendors can also pose a cybersecurity risk such as an employee of the vendor misusing Firm data or systems, or if the vendor becomes subject to a cybersecurity attack. Therefore, it is important for the Firms to perform a risk assessment and due diligence for all vendor relationships where we may outsource our Firm's data and systems in order to provide a service. As part of the Firm's risk assessment and on an ongoing basis (for critical vendors), the Firm will perform the following review.

- Perform pre-contract due diligence on prospective service providers;
- Perform ongoing due diligence on existing vendors;
- Establish contractual terms appropriate to the sensitivity of information and systems over which the vendor may have access. Contractual terms will govern the ongoing relationship and include controls for information protection after the relationship ends;
- Establish, maintain, and monitor vendor entitlements to Firm systems.

1.5.5.1 Due Diligence on Vendors

We may perform due diligence on our vendors in a variety of ways, but we prefer to use a risk based approach. This may include a discussion about the controls a vendor would need or has in place to remediate a weakness relative to our cybersecurity standards. For example, the Firm may expect a vendor to have the below required items in place depending on the risk level of the information to which the vendor has access to:

- Virus protection;
- Encryption of data while at rest or in transit;
- Business recovery practices;
- Change management processes;
- Ethical hacking of online systems;
- Limits on data access by vendor employees;
- Controls concerning sub-contractors; and
- System patch management.

As part of the Firm's due diligence on vendors, the Firm will also review our vendor contracts to ensure privacy and security regarding confidential client information. Below are some contractual elements the Firms may look for in conducting its review:

- Non-disclosure/confidentiality agreements specifying how sharing of information will be disclosed and/or limited;
- Data storage, retention and delivery. Contracts should specify how Firm data will be stored and transmitted while on a vendor's system such as encryption requirements, type and location of servers and business recovery practices;
- Breach notification responsibilities to address the manner and timing of the vendor's notification to the data owner of a security breach and who is responsible for notifying customers;
- Right to Audit Clauses giving the Firm the ability to perform physical audits of the vendor's data storage facility and controls;
- Vendor employee access limitations defining which vendor employees have access to Firm data;
- Use of subcontractor's language outlining any subcontractors that are used by the vendor and what access to data they would have; and
- Vendor Obligations upon termination including requirements that Firm data stored at the vendor's locations would be returned or destroyed and, if destroyed, how quickly it would be disposed of and how.

As part of the Firm's ongoing due diligence of vendors to ensure customer or Firm data is protected, we will determine which ongoing due diligence is necessary based on which vendors pose more risk due to them having access to more sensitive data or Firm systems which would require a higher level of scrutiny. The Firm's may perform onsite visits, send questionnaires verifying that vendors have the appropriate controls in place, etc. to ensure vendors are providing the appropriate security measures per the contract.

1.5.6 Technical Controls & Identity and Access Management

Our Firm has technical controls in place to protect the Firm software and hardware that stores and processes data, as well as the data itself. Technical controls we have in place are for authentication for access to systems, penetration testing, data encryption, wireless internet access, disposal of electronic data storage devices, loss of electronic devices, remote access, detecting unauthorized use, and loss of an electronic device.

1.5.6.1 Authentication Practices

The Firm has specific controls in place to limit users' access to a Firm's systems and data based on the role they perform within our Firm. This is an important area as this applies internally to employees, customers, and vendors. The Firm and its IT department only grants entitlement access to the Firm's systems based on the role the user performs in order to protect sensitive client or Firm information. The request for access is reviewed at the time of hire, upon a change in roles within the Firm, and/or periodically in the event that an individual's title or department changes. The forms of authentication that are required by our customers or employees to access electronic data storage devices which allow access to client communications and/or client information may include: user name/password, key FOBS/Secure IDs, challenge questions, fingerprint scan, other authentication.

For any persons who terminate from the Firm, the termination checklist should be completed which will ensure the Firm terminates the access to systems and information to which access is no longer appropriate.

1.5.6.2 Disposal of Electronic Data Storage Devices

The Firm requires that each associated person who possesses an electronic data storage device that he/she uses to conduct Firm business and will no longer be used dispose of the data contained on the device properly. If any confidential client information is contained on the

device. In the event the associated person wishes to dispose of a personal device, they must notify their Designated Principal or a person on the IT team to ensure the destruction of information on the device is handled according to this policy.

1.5.6.3 Detecting Unauthorized Activity on Networks or Devices

If the Firm or its technology department is alerted that unauthorized activity has occurred on a Firm network or a device, the Firm will immediately attempt to isolate the incident from where it occurred which may include terminating and/or freezing access, a customer account, a transaction, or an investment banking transaction. The Firm's IT department or Designated Principal will document the intrusion or activity that has occurred, attempt to determine how it occurred and document steps taken to resolve the incident.

1.5.6.4 Loss of Electronic Devices

In the event an electronic device that contains Firm or Client data is lost or stolen, the Associated Person must notify their Designated Principal immediately. The Designated Principal will meet with the Associated Person and risk assessment team to determine the type of client information that may be contained on the device. The Designated Principal will document the incident and contact customers if needed to alert them of their information being lost or compromised.

1.5.6.5 Remote Access

In addition to wireless technological advances that may raise concerns regarding the security of customer information, remote access to corporate networks through VPNs or other technology may raise similar concerns. As mentioned above, each year, more employees are taking advantage of alternative working arrangements by working from home and also working while traveling. While some employees may use wireless connections, others access corporate networks remotely through physical wire connections. Physical connections to corporate networks present similar concerns as Wi-Fi connections, although the Firm's can more easily address some of these concerns through the use of firewalls, routers, filters, and other means to guard against intrusion. The Firm has controls in place to require associated persons to request access to customer information on the Firm's server when accessing that information remotely.

1.5.6.6 Wireless Fidelity (Wi-Fi)

One relatively recent advance in technology is the use of Wi-Fi. There are at least two major issues that the Firm considers when allowing Associated Persons to use wireless technology when conducting Firm business. The first is that the data is broadcast out into the airwaves, thus making any confidential information in that data easier to intercept than if the user were required to connect via a physical wire. This is why the use of appropriate safeguards, for example encryption, is important to help prevent unauthorized parties from accessing data. Another issue raised by the use of Wi-Fi is that wireless connections present an attractive mechanism for hackers to tap into the user's workstation to gain access to a corporate network. A corporate network's protective measure (e.g., firewalls and similar defensive software) could be by-passed under such circumstances because, when a user connects a workstation directly to the Internet, the workstation itself becomes the connection point, without the benefit of all the protections available to a corporate network. Every workstation connected directly to the Internet creates a separate opportunity for intrusion. If an associated person intends to work remotely via access to Wi-Fi, they must only use a secured network which requires an authentication or a password.

1.5.6.7 Antivirus Software

The Firm utilizes antivirus software that must be installed on every Firm computer within our office. We require that each person perform routine updates to their antivirus software no less than monthly or automatically.

1.5.6.8 Use of Data Encryption

The Firm may consider using encryption technology, such as Information Rights Management or other software, which provides encryption for unstructured data elements such as PDF files and spreadsheets. Using encryption software provides protection over the file content as well as control over how the file contents can be used by those granted access to the data. Senior management will address who should use encryption, how to securely distribute encryption software or keys, as well as how to rotate keys or when someone should be added as a user. The Firm's management may also determine if encryption technology is required on devices that access confidential client information such as computers, tablets, smartphones, or other electronic devices.

1.5.6.9 Use of Firm Websites to Access Client Data

The Firm has a password protected link on our website for an associated person to access pertinent resources. No items on our password protected site have any private client data. If we decide to store client sensitive data on our website, we use SSL or other encryption on the website. Any client portals links on our Firm websites will use SSL or other encryption to protect data.

1.5.7 Cyber Intelligence and Information Sharing

The Firms will use cyber threat intelligence to improve our ability to identify, detect, and respond to cybersecurity threats. We may assign responsibility for cybersecurity intelligence gathering and analysis at the organizational or individual levels, establish mechanisms to disseminate threat intelligence and analysis rapidly to appropriate groups within the Firm, evaluate threat intelligence from tactical and strategic perspectives, determine the appropriate time frame for the course of action, and/or participate in information sharing with other organizations such as the FS-ISAC. By the Firm using cybersecurity intelligence and information sharing, we can reduce our vulnerability to cybersecurity threats and improve our ability to protect Firm and customer information. Our Firm may rely on vendors to provide a range of cybersecurity services, including threat intelligence analysis, which would include information about shared software vulnerabilities, identifying common exposures relative to the Firm's technology, performing network analysis to identify anomalous activity, and conducting vulnerability and penetration testing.

However, if the Firms decide to perform cybersecurity intelligence internally, the Firm may rely on a broad range of sources such as centralized information sharing centers, industry peers, cybersecurity information vendors, software vendors, and government and law enforcement agencies.

When the Firms review any cybersecurity threats or intelligence, our AMLCO and Information Security Committee will review the information to determine if any of the threats pose a risk to our Firm. If we determine the threat is a risk, the Firm will take the necessary steps to protect our Firm's systems and customer data. Documentation of the Firm's efforts to eliminate any threat or risk will be evidenced in the Firm's cybersecurity intelligence files.

1.5.8 Cyber Security Training

The importance of cybersecurity training is widely recognized and a critical piece of an organization's infrastructure. All Associated Persons using Firm systems should be informed, trained, and understand their specific roles and responsibilities. This includes educating Associated Persons of the risks associated with the data they may encounter when performing their jobs. The Firm may provide training throughout the year as needed to inform the Firm and its associated persons of changes in technology, technology updates, cyber security threats, etc. The training may be delivered in a variety of methods, which may include but are not limited to: webcast, email delivery of documents, videos, etc. Regardless of when and how the training is provided, it will generally be documented in the Firm's training plan or on an as-needed basis.

1.6 Managing a Privacy Breach

If any person associated with the Firm detects or become aware of any breaches to the Firm's electronic or paper records that could comprise confidential information, he or she must immediately notify the AMLCO. The AMLCO shall investigate any reported breaches and report to the Information Security Committee to take the following actions, as appropriate:

1. To the extent possible, identify the information that was disclosed and the improper recipients;
2. To the extent possible, categorize the incident based on operational impact and sensitivity of information involved;
3. Take any actions necessary to prevent further improper disclosures;
4. Take any actions necessary to reduce the potential harm from improper disclosures that have already occurred;
5. Consider discussing the issue with counsel, state or federal regulatory authorities and/or law enforcement officials;
6. Evaluate the need to notify affected clients and make any such notifications;
7. Collect, prepare, and retain documentation associated with the inadvertent disclosure and the Firm's response(s), including post-incident review of events and actions taken, if any; and
8. Evaluate the need for changes to the Firm's privacy protection policies and procedures in light of the breach.

1.6.1 Cyber-Attack

If we determine that a customer's account or Firm systems have been attacked, the AMLCO will conduct a timely investigation to determine the extent of data or monetary loss and identify root cause(s). The AMLCO will log all information to be recorded and maintained to retain details surrounding the cybersecurity attack and report to the Information Security Committee. In the event of an attack, the Firm will perform the following activities:

- Contact FINRA, SEC, states and other regulatory authorities immediately in accordance with Rule 4530(b) and report material cyber incidents that do not trigger a reporting obligation to our Regulatory Coordinator at FINRA.
- Monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
- Alert others in the Firm (including the Firm's Legal and Compliance Department, if applicable) to be mindful of unusual activity in other customer accounts.

- Identify, if possible, the root cause of the account intrusion (e.g., the Firm's system was compromised, the individual account was hacked, the customer was the victim of identity theft) and determine whether the intrusion is isolated to one account.
- Notify third party custodians (if applicable)
- Notify third party vendors as required by contracts
- If appropriate, contact law enforcement agencies, such as the FBI or, if the U.S. mail is involved, the United States Postal Inspector.
- If the Firm has not already done so, contact the customer and, if appropriate, change the password and/or account number.
- Determine whether any unauthorized person has gained or potentially has gained access to an account holder's personally identifiable information and, if so, whether the Firm must provide a specific type of notification to the customer or others under state law regarding the loss of the customer's information. Some states may require notice to the State Attorney General or other state law enforcement agencies in addition to customer notification.
- Determine whether the Firm should file a Suspicious Activity Report (SAR) under the federal anti-money laundering provisions.
- If there is a monetary loss to customers or a customer's information is stolen, determine if the Firm wants to offer free credit monitoring or reimburse clients who lost money through the attacks.

1.7 New Technology

Periodically our Firm will update our technology and use new and different methods of communication, whether through the use of wireless technology, new software/systems, or allowing employees to work remotely. However, the use of new technology or updates to technology can also pose a risk to our Firm and customers are protected.

1.7.1 Use of Cloud Services

The use of cloud services can present a challenge to our Firm's cybersecurity efforts because they can enable a business unit within our Firm to pursue a substantial technology initiative with minimal involvement from the technology or other departments that traditionally have been involved in vetting and approving vendor relationships and that could act as a control to ensure that sound cybersecurity practices are in place. Secondly, cloud based services along with other outsourced information technology service can blur the boundary between our Firm and non-Firm systems and can make it challenging for the Firm to define the perimeter of our technology environment and establish appropriate controls.

As part of our due diligence for a cloud service provider, the Firms will consider authentication and access control to the data, how the vendor controls access to the system and data stored, what processes are used to approve requests to gain access, what controls are in place to prevent the hacking of the systems, what types of secure coding practices does the vendor enforce, and who has access to the vendor's data center.

1.8 Business Continuity

In the event of a business disruption that may occur from a cyber-attack, intrusion, or unauthorized access, the Designated Principal or assignee will document the business disruption that occurred, how it occurred, the type of disruption it caused, and whether the Firm needed to implement the Firm's business continuity plan. If, after implementing of the business continuity plan, the Firm determines that changes are needed to the plan, the CCO will be responsible for making those changes.

1.9 Cyber Insurance

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. While it is not a requirement for the Firms to maintain cyber-insurance; some financial institutions today take out coverage to protect them from losses. The AMLCO and Information Security Committee will review the need for cyber-insurance no less than annually, to determine whether, based on risk factors, etc., obtaining cyber-insurance is appropriate and necessary. Some factors considered in a cyber-insurance policy review include:

- liability limits for data breaches;
- remediation cost reimbursement limits to respond to breaches, and;
- coverage for regulatory and legal fines and penalties.

Privacy Policy/Regulation S-P

Name of Supervisor ("designated Principal"):	Designated Principal, CCO
Frequency of Review:	In daily course of business
How Conducted:	Privacy notice process Review RR activity/correspondence Customer file reviews Enforce information security procedures; train personnel in information protection
How Documented:	Privacy notices, opt out records. Account information Records of monitoring and testing, if required, of internal systems; ensure and document third party monitoring/testing of systems, if applicable. Incident Response Policy Firm WSP / Compliance Procedures
WSP Checklist:	SEC Regulation S-P (As amended in 2024/effective 12/3/2025), SEC Regulation S-ID, Notices 00-66, 05-49; Graham-Leach Bliley Act, as amended
Comments:	Also reference Business Continuity Plan for technical details on document back-up and the Firm's Cybersecurity and ID Theft Prevention Program, if applicable.

Reg S-P requires the Firm to provide its individual clients with notices describing its privacy policies and procedures. These privacy notices must be delivered to all new individual clients upon entering into an agreement, and at least annually thereafter. Reg S-P does not require the distribution of privacy notices to companies or to individuals representing legal entities. In addition to Reg S-P, certain states have adopted consumer privacy laws that may be applicable to the Firm with clients who are residents of those states.

The Company has adopted procedures in a separate "Incident Response Plan" Reg. S-P as amended on December 3, 20254. The purpose of this policy is to establish a formal framework for detecting, responding to, and recovering from cybersecurity incidents involving unauthorized access to or use of customer information. In instance where you have a question regarding the firms procedures, reach out to Compliance or Technology leadership for information and guidance.

The Firm's view protecting private information regarding its clients and potential clients as a top priority. Pursuant to the requirements of the Gramm-Leach-Bliley Act (the "GLBA") and guidelines established by the Securities Exchange Commission regarding the Privacy of Consumer Financial Information (Regulation S-P), the Firm has instituted the following policies and procedures in an effort to ensure that such nonpublic private information is kept private and secure.

Associated Persons will maintain the confidentiality of information acquired in connection with their employment, with particular care being taken regarding Nonpublic Personal Information. Improper use of the Firm's proprietary information, including Nonpublic Personal Information, is cause for disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities.

The Firms will seek to limit its collection of Nonpublic Personal Information to that which is reasonably necessary for legitimate business purposes. The Firm's will not disclose Nonpublic Personal Information except in accordance with these policies and procedures, as permitted or required by law, or as authorized in writing by a client. The Firms will never sell Nonpublic Personal Information.

With respect to Nonpublic Personal Information, the Firm will strive to: (a) ensure the security and confidentiality of the information; (b) protect against anticipated threats and hazards to the security and integrity of the information; and (c) protect against unauthorized access to, or improper use of, the information.

Although these principles and the following procedures apply specifically to Nonpublic Personal Information, Associated Persons must be careful to protect all of the Firm's proprietary information.

2.1 Information Practices

The Firm's limit the use, collection, and retention of client or potential client information to what the Firms believes is necessary or useful

to conduct its business or to offer quality products, services, and other opportunities that may be of interest to its clients or potential clients.

2.1.1 Disclosure of Nonpublic Personal Information

Associated Persons should take reasonable precautions to confirm the identity of individuals requesting Nonpublic Personal Information. Associated Persons must be careful to avoid disclosures to identity thieves, who may use certain Nonpublic Personal Information, such as a social security number, to convince an Associated Person to divulge additional information. Any contacts with suspected identity thieves must be reported promptly to the Designated Principal.

1. Each Associated Person has a duty to protect Nonpublic Personal Information of clients collected by the Firm.
2. Each Associated Person has a duty to ensure that Nonpublic Personal Information of the Firm's clients is shared only with Associated Persons and others in a way that is consistent with the Firm's Privacy Notice and the procedures contained in this Policy.
3. Each Associated Person has a duty to ensure that access to Nonpublic Personal Information of the Firm's clients is limited as provided in the Privacy Notice and this Policy.
4. No Associated Person is authorized to sell, on behalf of the Firm or otherwise, Nonpublic Personal Information of the Firm's clients.

Associated Persons with questions concerning the collection and sharing of, or access to, nonpublic personal information of the Firm's clients must look to the Designated Principal for guidance.

In certain circumstances, Regulation S-P permits the Firm to share Nonpublic Personal Information about its clients with non-affiliated third parties without providing an opportunity for those individuals to opt out. These circumstances include sharing information with a non-affiliate (1) as necessary to effect, administer, or enforce a transaction that a client requests or authorizes; (2) in connection with processing or servicing a financial product or a service a client authorizes; and (3) in connection with maintaining or servicing a client account with the Firm.

Nonpublic Personal Information may only be provided to third parties under the following circumstances:

1. To accountants, lawyers, and others as directed in writing by clients;
2. To specified family members as directed in writing by clients, or as authorized by law;
3. To third-party service providers, as necessary to service client accounts; or
4. To regulators and others, as required by law.

To the extent practicable, Associated Persons will seek to remove nonessential Nonpublic Personal Information from information disclosed to third parties. Social security numbers must never be included in widely distributed lists or reports.

Prior to providing any third-party service provider with access to personal information about individual clients who are residents of Massachusetts, the Firm will require, by contract, third-party service providers who may have access to such clients' information, to implement and maintain appropriate security measures to protect such clients' personal information consistent with Massachusetts Standards for Protecting Personal Information (201 CMR 17.00) and any applicable federal regulations.

2.1.2 Service Providers

When the Firm is not comfortable that service providers (e.g., attorneys, auditors, and other financial institutions) are already bound by duties of confidentiality, the Firm requires assurances from those service providers that they will maintain the confidentiality of Nonpublic Personal Information they obtain from or through the Firm. In addition, the Firm selects and retains service providers that it believes are capable of maintaining appropriate safeguards for nonpublic information, and the Firm will require agreements from its service providers that they will implement and maintain such safeguards.

2.1.3 Processing and Servicing Transactions

The Firms may also share information when it is necessary to effect, administer, or enforce a transaction requested or authorized by clients. In this context, "necessary to effect, administer, or enforce a transaction" includes what is required or is a usual, appropriate, or acceptable method:

1. To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the client's account in the ordinary course of providing the financial service or financial product;
2. To administer or service benefits or claims relating to the transaction or the product or service of which it is a part; or
3. To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the client or the client's agent or broker.

2.1.4 Sharing as Permitted or Required by Law to Non-Affiliated Third Party

The Firms may disclose information to non-affiliated third parties as required or allowed by law. For example, this may include disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, or an audit or examination.

2.2 Privacy Policy Notice

The Firms have developed a Privacy Notice, as required under Regulation S-P, to be delivered to clients. The notice discloses the Firm's information collection and sharing practices and other required information. The notice will be revised as necessary any time information practices change.

2.2.1 Privacy Notice Delivery

The Firm's clients must receive a copy of the Firm's Privacy Notice at certain points in the -client relationship.

2.2.1.1 Initial Privacy Notice

As regulations require, all new clients receive an initial Privacy Notice at the time the client relationship is established (i.e., upon execution of the agreement for services).

2.2.1.2 Annual Privacy Notice

The Firms only provides Nonpublic Personal Information to non-affiliated third-parties as permitted by the following exceptions:

1. To accountants, lawyers, and others as directed by the client;
2. To specified family members as directed by clients or as authorized by law;
3. To a third-party service provider, as necessary to provide services requested or authorized by the client;
4. To a third-party service provider who performs services for the Firm pursuant to an agreement prohibiting disclosure of client information, except as necessary to perform the services;
5. To regulatory authorities and others, as required by law.

Accordingly, the Firm will not be required to provide an Annual Privacy Notice to a client unless it has changed its privacy policies since the Privacy Notice was last provided to the client. In any year in which the Firm either changes its privacy policies or discloses Nonpublic Personal Information to non-affiliated third-parties outside of the exceptions described above, then it will send an Annual Privacy Notice to its clients.

The Designated Principal oversees the distribution of the initial and any required annual Privacy Notices and will maintain a record of the dates of delivery and the identification of recipients of annual Privacy Notices.

2.2.1.3 Revised Privacy Notice

If there is a change in the Firm's collection, sharing, or security practices, Regulation S-P requires that the Firm amend its Privacy Policy and promptly distribute a revised Privacy Notice to existing clients.

2.2.1.4 Joint Relationships

If two or more individuals jointly obtain a financial product or service from the Firm, the Firm may satisfy the initial, annual, and revised notice requirements by providing one notice to those individuals jointly.

IDENTITY THEFT WORKSHEET

Client Identity Theft Red Flag/Prevention/Mitigation

The Firm has identified the following red flags that should be considered by its Associated Persons in the opening and maintenance of covered accounts.

	Client Account ID Theft- Red Flags
	Electronic communication received when client does not typically communicate electronically
	PII has been compromised or exposed or is associated with fictitious information
	Client has been the victim of a breach of information
	Unauthorized activity has occurred or been attempted in the client's account
	Identification and/or documentation presented appears to be altered or forged, or has inconsistencies between what is being presented and what is being stated

For Red Flags observed or detected during account opening the Associated Person will take steps outlined below, as appropriate to the type and seriousness of the threat:

	Client Account- ID Theft Prevention
	Verify the application. Verify the applicant's collected information (for example: name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
	Review government identification. Review a government-issued identification documentation (for example: a driver's license or passport).
	Seek additional verification. In certain circumstances, it may be important to conduct additional verification, including, but not limited to: a. Contacting the customer; b. Checking references with other affiliated financial institutions; or c. Obtaining a financial statement.
	Deny the application. In circumstances where verification cannot be obtained, the application should result in denial.
	Escalation. When the applicant is suspected of using an identity other than their own, immediately report the matter to the AMLCO and complete the HF029 Preliminary Suspicious Activity Report for review to include a description of the situation, stating the account number, effective date, how the incident was discovered, who discovered the incident, when and where the incident occurred. To the extent possible the AMLCO will: a. Identify the information that was disclosed and improper recipients; and b. Categorize the incident based on the operational impact and sensitivity of info involved.

Where Red Flags are raised when someone is seeking to access an existing Client's account, consider the following options:

	Client Account- ID Theft Mitigation
	Monitor, limit, or temporarily suspend activity in the account until the Red Flag is resolved
	Contact the Client to determine if there has been an attempt at Identity Theft.
	Check related accounts. Review the client relationship to determine if additional attempts have been made, without authorization.
	Deny the application. In circumstances where verification cannot be obtained, the application should result in denial.
	Escalation. When the applicant is suspected of using an identity other than their own, immediately report the matter to the AMLCO and complete the HF029 Preliminary Suspicious Activity Report for review to include a description of the situation, stating the account number, effective date, how the incident was discovered, who discovered the incident, when and where the incident occurred. To the extent possible the AMLCO will: a. Identify the information that was disclosed and improper recipients; and b. Categorize the incident based on the operational impact and sensitivity of info involved.

Associated Person Identity Theft Red Flag/Prevention/Mitigation

Email hacking and technology intrusions take place throughout the world. Malicious email may introduce malware-ransomware to infect your system and may delete or encrypt your files or capture confidential information.

For this reason, the Firms require enabling email 2-step authentication. This extra step requires a code to log into your email or whenever account settings are changed.

	Associated Person Malicious Email Red Flags
	"From" Line- Sender appears to be someone you know, but is a spoof. Ex: Real Email: admin@harborfs.com; Spoofed Email: admin@harberfs.com
	"To" Line- Email is sent to multiple people you do not recognize, but you are being cc'd
	Hyperlinks- Be cautious of embedded links. Hover your mouse to see the destination URL. Confirm source is trusted before opening.
	Time- Consider the time you received the email and if it is normal.
	Subject- Fishy subject line examples: "Need wire transfer now"; "Change password immediately". Validate the source before taking any action.
	Attachments- Never open attachments you are not expecting. File types such as .exe or a duplicate file type such as .xls.xls should not be downloaded or opened.
	Content- Email urging you to update information or change your password in order to avoid consequences is often a hacking trick. In addition, if there are grammar or spelling errors, confirm source is legitimate.

If an Associated Person suspects the email is suspicious, delete it and send it to trash. Never click the "unsubscribe" link in suspicious email. If an Associated Person thinks the request may be legitimate but is unsure, contact the sender any other way besides using the "reply" option.

	Associated Person Signs of Email Intrusion
	Associated person receives unexpected reply(ies)/request for more information to an email they did not originate
	Associated Person realizes they have inadvertently opened an executable file from an unknown source
	Associated Person realizes they responded to a suspicious email with a link to change a password
	Email outbox has sent emails not originated by the Associated person
	Read/unread status shows messages have been read that the Associated Person does not recall reading
	Sent email requests for password resets for sites Associated Person doesn't remember sending
	Associated person finds redirected emails in their junk, trash or delete email folders

Associated persons must immediately report to their Designated Principal if they suspect their business email has been compromised or if they suspect malware/virus on their information technology equipment used for business. The first thing a hacker typically does is change your passwords.

	Associated Person Email Intrusion Escalation
	When someone other than the Associated Person is suspected to be using the Associates business email, immediately escalate the matter to the AMLCO and complete the HF029 Preliminary Suspicious Activity Report for review to include a description of the situation, stating the account number, effective date, how the incident was discovered, who discovered the incident, when and where the incident occurred.
	Confirm Level Four Financial has reset the email password.
	Scan the computer and other devices for viruses/malware. Changing passwords without cleaning the system might not lock out hackers.
	Inform your email contacts they "should not open any emails or click any links" from you that look suspicious and to check their own accounts if they did open.
	Use a third-party website to do a check for compromised email.
	Check your email signature, 'reply to' email address and your sent folder. Eliminate any unusual rules or email accounts you don't recognize.
	Continue to monitor your information and your client accounts for suspicious activity and report to the AMLCO
	Associated person finds redirected emails in their junk, trash or delete email folders

AMLCO Review

The AMLCO may take the following additional steps to protect the clients and the Firm as described in Section 1.6 Managing a Privacy Breach. In addition, the AMLCO may consider the following:

1) Use a third-party website to do a check if the Associates email has been compromised. (Ex: Have I Been Pwned?)
2) Report an email breach to the Firm's Email provider. Request the provider investigate user's operating system, mobile device type, and the Internet Protocol (IP) address of suspicious email.
3) Consider creating a new Associate email account.

Identity Theft Training

Training plays an important role in the prevention, detection and response to Identity Theft, as well as decreasing the risks faced by the Firm. The Firm will provide training on an annual basis for its Associates, Affiliates, and any parties that are in contact with accounts.