Information Security Plan

Developed by:
Iota Finance LLC
32469 Jefferson Drive
Solon, Ohio 44139
(216) 200-8135
Hello@Iota-Finance.com

Information Security Plan

Iota Finance LLC, hereby referred to as "the firm," developed and implemented an information security plan (ISP) to create effective administrative, technical and physical safeguards for the protection of client information. This ISP sets forth procedures for evaluating and addressing the electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting client information.

101) *Designation of representatives:* The Managing Partner is designated as the person who shall be responsible for coordinating and overseeing the ISP. This person is hereby referred to as the "representative." The designated representative may assign or delegate other representatives of the firm to oversee and coordinate elements of the ISP. Any questions regarding the implementation of the ISP or the interpretation of this document should be directed to the representative or his or her designees.

102) *Risk identification and assessment and current safeguards*: The firm has identified, as part of the ISP, the internal and external risks to the security, confidentiality and integrity of client information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and implemented the following safeguards for controlling these risks:

1. **Multifactor authentication (MFA)**: *The use of two or more authentications such as pin/password/biometric/token are used when available with our vendors. Client sensitive financial, banking, and tax information are always secured through MFA. We only work with vendors who provide MFA for said sensitive information, additional information on our vendor selection process can be found in §104.*

2. **Least amount of access**: *The least amount of access necessary is given to specific client files/folders and environments. Firm staff and contractors are only given access to client files on an as-needed basis. All access permissions are documented and reviewed at least annually.*

3. **Data loss prevention (DLP)**: *Data is controlled, recorded and monitored as it moves through the organization. We maintain regular backups of client files on separate operating systems and servers.*

4. **Network access restrictions**: *Firewalls are used with all network interactions and a virtual private network (VPN) is required for all out-of-office internet use to ensure only managed and controlled devices/environments have access to client data. All firm computers have BitDefender suite products installed, including firewall, anti-malware, anti-spyware, anti-adware, and multi-layer ransomware protection.*

5. **Encryption**: *Anything that stores, transmits or accesses client data is encrypted. We maintain this policy across all firm devices and disallow the use of external storage devices. All firm files and data are stored and backed up on remote servers on a regular basis.*

103) *Design and implementation of safeguards program*: The risk assessment and safeguard control policies described above shall apply to all methods of handling or disposing of client information, whether in electronic, paper or other form. The representative will, on a regular basis, implement safeguards to control the risks identified through such assessments and regularly test or otherwise monitor the effectiveness of such safeguards in relevant areas of the firm's operations, including:

1. **Employee management and training**: The representative will evaluate the effectiveness of the firm's procedures and practices relating to access and use of client information. This evaluation will include assessing the effectiveness of the firm's current policies and procedures in coordination with relevant departments, as appropriate, as well as adequate training of employees. Procedures include:

    a) All firm employees and contractors must pass a background criminal background check and provide at least two verifiable references that can speak to their performance and aptitude.
    b) All firm employees have individual, monitored, accounts. All employees are required to use surge protectors and/or uninterruptible power supplies. Firm computers come with BitDefender cybersecurity licenses, coupled with MFA.
    c) Employee and contractor information security protocols are adopted above (§104) and through the recommendations of IRS Publication 4557 and NISTIR 7621.
    d) Employees and contractors are required to participate in a firm-designed initial aptitude assessment on current tax law or they are required to participate in trainings covered by the firm.

2. **Information systems**: The representative will assess the risks to financial information associated with the firm's information systems, including network and software design, information processing and the storage, transmission and disposal of financial information. The representative will coordinate with relevant departments, as appropriate, to assess the following procedures:

    a) All firm computers are updated regularly to the latest version of their operating systems, cybersecurity softwares, drivers, and general applications to ensure data integrity.
    b) Old firm hardware is disposed of in secure recycling programs provided by local vendors. All backups are stored in off-site cloud storage to ensure security and safety.
    c) The firm follows a Document Retention Policy, accompanied by a regularly-updated Document Retention Exceptions Log to ensure accountability.
    d) The firm is covered by a Cyber Security policy through Camico, in the event of disasters and information security incidents.

3. **Detecting and managing system failures**: The representative will evaluate procedures and methods of deferring, detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. The representative may elect to delegate the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the firm, and will coordinate with relevant departments, as appropriate. Procedures include:

    a) The firm will conduct annual internal audits on cybersecurity processes and softwares as a proactive measure to minimize cybersecurity and information technology incidents.
    b) Monthly reviews of security scans, attempted unauthorized accesses, and other unusual or suspicious activities will be conducted to ensure the integrity of the firm and its' clients sensitive information.

104) *Protocols to select service providers that can maintain appropriate safeguards:* The representative shall coordinate with those responsible for the third-party service procurement activities to raise awareness of, and to institute methods for, selecting and retaining only those service providers that maintain appropriate safeguards for client information. The representative will also oversee the handling of client information by third-party service providers as follows.

1. Find a local service provider;
2. Check the references of the potential service provider;
3. Provide the potential service provider a copy of the ISP and request a review of the ISP by the potential service provider;
4. Obtain a copy of the potential service provider's ISP as it relates to client data;
5. Confirm the potential service provider has experience with the firm's type of practice;
6. Inquire if the potential service provider has experience to support the firm's hardware and software; and,
7. Check for the potential service provider's certifications and partnerships with major manufacturers.

105) *Procedures for the evaluation and periodic adjustment of the ISP:* The representative will evaluate and adjust the ISP based on the risk identification and assessment activities undertaken pursuant to the ISP, as well as any material changes to the firm's operations or other circumstances that may have a material impact on the ISP as follows.

1. Conduct internal security risk assessments periodically through reviewing security logs and auditing software effectiveness; and,
2. Schedule and perform annual assessments of cybersecurity and software service providers to ensure continued compliance and responsiveness to inquires.