Information (Data) Security Plan[1]

[Note: CAMICO has created this *Information (Data) Security Plan* template for illustrative purposes only. Under the Gramm-Leach-Bliley Act's ("GLBA") Safeguards Rule,[2] a tax return preparer is required to create and enact an *Information (Data) Security Plan* to protect client data; the plan should be appropriate to the firm's size and complexity, the nature and scope of its activities, and the sensitivity of the client's information it handles. Accordingly, a firm's efforts to comply with the GLBA Safeguards Rule is an organization-specific initiative. As such, CAMICO recommends that each firm work with their IT/cyber specialists and legal counsel, as appropriate, to modify and tailor this template to ensure the firm's compliance with GLBA's Safeguards Rule and other applicable laws.]

<Firm> ("Firm" / "we" / "our" / "us") recognizes the importance of and is committed to creating effective administrative, technical, and physical safeguards to protect client information from unauthorized access. We are a certified public accounting Firm that provides <specify services: accounting, assurance, tax, financial advisory, and consulting services to businesses, non-profits, and individuals> (the "Services"). In the normal course of business, we receive clients' sensitive information, which may include social security numbers, tax identification numbers, bank account information, investment/brokerage statement numbers, and other confidential information.

In compliance with applicable federal and state laws, <Firm> has developed this *Information (Data) Security Plan* ("ISP"), which sets forth the Firm's policy and procedures for evaluating and addressing the electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting client information.[3]

Firm Governance and Compliance

The <Name of Position or Person> ("Firm Representative") is designated as the person who shall be responsible for overseeing and updating the ISP as needed. The Firm Representative reports directly to the <Specify: Managing Partner/Firm Executive Committee/etc.>. The Firm Representative may assign or delegate other Firm representatives to oversee and coordinate elements of the ISP. Any questions regarding the implementation of the ISP or with interpreting this document should be directed to the Firm Representative or his or her designees.

---

[1] CAMICO recommends that a firm work with their IT/cyber specialists and legal counsel as appropriate to develop and execute an *Information/Data Security Plan* that complies with the Gramm-Leach-Bliley Act's ("GLBA") Safeguards Rule and all other applicable laws.

[2] The Financial Services Modernization Act of 1999, commonly referred to as the Gramm-Leach-Bliley Act or GLBA, gives the Federal Trade Commission ("FTC") authority to set information safeguard regulations for various entities, including professional tax return preparers.

[3] IRS Publication 4557, Safeguarding Taxpayer Data (PDF), details critical security measures that all tax professionals should have in place. The publication also includes information on how to comply with the GLBA Safeguards Rule. A growing number of states have also enacted laws and/or issued regulations mandating businesses to adopt reasonable safeguards to protect personal information, and firms should consult with legal counsel in their state(s) to ensure compliance with all applicable laws.

The Firm Representative will verify compliance with this policy through various methods, including but not limited to, periodic walkthrough, monitoring, business tool reports, and internal <and external> audits. The Firm Representative will report all findings, regulatory and state security laws changes, and any other information technology security related matters directly to the <Specify: Managing Partner/Firm Executive Committee/etc.>.

Compliance with this policy is mandatory for all employees and independent contractors. Employees should notify their immediate supervisor or any member of management upon learning of violations of this policy and the supervisor and/or member of management will be responsible to notify the Firm Representative. Employees who violate this policy (including knowingly not notifying their supervisor or another member of Firm management of such violations) will be subject to disciplinary action, up to and including termination of employment.

Safeguards for the Protection of Client Information

Firm has made reasonable efforts to identify potential 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 compromises of such client information.

We have implemented the following safeguards for controlling risks associated with accessing, collecting, storing, using, transmitting and protecting client information, including the handling and/or disposing of client information, whether in electronic, paper or other form. The first six items (the "Security Six") were developed by the Internal Revenue Service as part of their "Taxes-Security-Together" Checklist:

"Security Six" Safeguards[4]

1. Anti-virus software and anti-malware software
<Provide organization-specific details and/or reference to Firm-specific policies and/or procedures.>

2. Firewalls for hardware and software
<Provide organization-specific details and/or reference to Firm-specific policies and/or procedures.>

3. Multi-factor authentication
<Provide organization-specific details and/or reference to Firm-specific policy and/or procedures.>

4. Back-up software/services
<Provide organization-specific details and/or reference to Firm-specific policy and/or procedures.>

5. Encryption
<Provide organization-specific details and/or reference to Firm-specific policy and/or procedures.>

6. Virtual Private Network ("VPN")
<Provide organization-specific details and/or reference to Firm-specific policy and/or procedures.>

[4] The firm needs to include organization-specific information describing the details relevant to each of the six safeguards noted. Refer to the IRS website for detailed guidance at https://www.irs.gov/newsroom/tax-security-2-0-a-taxes-security-together-checklist-step-1. Procedures may be updated more frequently than policies to reflect changes in business processes and technology.

Other Safeguards

7. Passwords
    a. All computer users at the Firm will have their own account and password.
    b. Firm requires passwords to be at least eight characters (including capital and lower-case letters, numbers and symbols). Personnel will be prompted and required to update their passwords every <specify frequency>.
    c. Firm expressly prohibits the sharing of accounts and/or passwords with others.

8. The Firm maintains the following policies which are incorporated by reference into this document as they support the Firm's commitment to creating effective protocols for protecting client information:
    a. *Record Retention and Destruction Policy* (last updated on <specify date>), which sets forth the Firm's protocols and procedures for the protection and physical security of all hard-copy files, electronic files, computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.
    b. *Confidentiality Policy* (last updated on <specify date>), which sets forth the nature and extent of the obligation of Firm members to hold in strict confidence all client-related information.
    c. *Incident Response Plan*[5]
    d. <Specify other applicable Firm policies related to Privacy, Computer/IT Security, Mobile Devices, Access and Use Agreement, etc.>

9. Cyber insurance coverage
    a. The Firm maintains insurance coverage for <specify: first-party and/or third-party> cyber matters. Questions regarding insurance coverage, cyber resources, and/or the requirements for reporting matters to the insurance carrier(s) should be directed to Firm Representative.

10. Third-party service providers[6]
    a. The Firm Representative is responsible for overseeing and monitoring compliance with the Firm's procedures and safeguards for the sharing of client information with third-party service providers. We maintain internal procedures and safeguards to protect the confidentiality of client information and, as such, it is the Firm's protocol to secure confidentiality terms with all service providers and to take reasonable precautions to determine that they have appropriate procedures in place to prevent the unauthorized release of client confidential information to others. If the Firm is unable to obtain appropriate confidentiality terms with a third-party service provider, prior to the release of any confidential client information to such third-party service provider the Firm will require written client consent.

11. <Specify other applicable Firm safeguards.>

[5] The GLBA Safeguards Rule requires that a plan be in place for responding effectively to security breach threats. CAMICO recommends that firms have an *Incident Response Plan* for this purpose, which can be incorporated by reference in this ISP. This template should be modified as appropriate if the firm does not have an *Incident Response Plan*. See Footnote 7.

[6] If the firm has a written policy in place regarding third-party service providers, it should be incorporated by reference in this ISP and this section modified accordingly.

FTC's Safeguard Rules Checklist

In addition to the safeguards noted above, the Firm Representative is also responsible for monitoring and updating the Firm's *Safeguards Rule Checklist,* which is incorporated by reference in this ISP in the Addendum. The *Safeguards Rule Checklist* tool was disseminated by the FTC, promulgated by the IRS in *Publication 4557, Safeguarding Taxpayer Data (Rev. 6-2018),* and adopted for use by the Firm. The tool is designed to help track the Firm's compliance efforts with three additional key areas of risk that are important as it relates to information security in relevant areas of our operations: Employee Management and Training, Information Systems, and Detecting and Managing System Failures.

Employee Management and Training

All Firm Partners/Shareholders, Managers, Supervisors and Seniors are tasked with supporting the Firm Representative to ensure that all personnel are aware of and comply with this ISP and other applicable policies and procedures. This includes, but is not limited to, developing and applying appropriate performance standards, training curriculum, and control practices and procedures designed to provide reasonable assurance that all employees understand and support the Firm's commitment to safeguarding client information. Refer to the Firm's responses to specific compliance efforts noted on the Firm's *Safeguards Rule Checklist.*

Information Systems

The Firm Representative works closely with the Firm's technology team to assess and mitigate through applicable policies and procedures the risks associated with the Firm's information systems, including network and software design, information processing, and the storage, transmission and disposal of client information. Refer to the Firm's responses to specific compliance efforts noted on the Firm's *Safeguards Rule Checklist.*

Detecting and Managing System Failures

The Firm takes reasonable steps to deter, detect and defend against security breaches as noted on the *Safeguards Rule Checklist*. In addition, the Firm has an *Incident Response Plan*[7] that addresses protocols in the event of a suspected breach to ensure timely and appropriate responsiveness.

Future Updates

In consideration of our Firm's size and complexity, the nature and scope of the professional services we render to our clients, and the sensitivity of the information we collect, the Firm has determined that compliance with this ISP appears to satisfy the current regulatory and legal requirements.

[7] As referenced in Note 5, the GLBA Safeguards Rule requires that a plan be in place to respond appropriately and effectively to security breach threats. CAMICO recommends that firms have an *Incident Response Plan* for this purpose, which can be incorporated by reference in this ISP. If a firm does not have an *Incident Response Plan*, then this template should be modified as appropriate and additional information regarding the firm's procedures should be added to the ISP and/or detailed in the *Safeguards Rule Checklist*.

The Firm Representative will periodically review the effectiveness of the program with <specify: Managing Partner/Firm Executive Committee/etc.> and will reassess the risk factors as well as any material changes to the Firm's operations and recommend changes to the ISP as necessary. Subsequent updates to the ISP will be communicated to all employees in accordance with Firm protocols.

Addendum: Safeguards Rule Checklist

The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operation, including three areas that are particularly important to information security: Employee Management and Training; Information Systems; and Detecting and Managing System Failures.

Not each of these recommendations will apply to circumstances found in tax preparer offices, but they still provide a good guide for the creation of a security plan and reinforce IRS recommendations that tax professionals establish strong security protocols. The following checklist is from the FTC (Source: https://www.irs.gov/pub/irs-pdf/p4557.pdf).

Employee Management and Training

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Following are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal.

Ongoing	Done	N/A	
			The success of your information security plan depends largely on the employees who implement it. Consider these steps:
☐	☐	☐	Check references or doing background checks before hiring employees who will have access to customer information.
☐	☐	☐	Ask every new employee to sign an agreement to follow your company's confidentiality and security standards for handling customer information.
☐	☐	☐	Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
☐	☐	☐	Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers, and symbols.) **(*IRS suggestion:* passwords should be a minimum of eight characters.)**
☐	☐	☐	Use password-activated screen savers to lock employee computers after a period of inactivity.
☐	☐	☐	Develop policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.

Ongoing	Done	N/A	
			Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
☐	☐	☐	• Locking rooms and file cabinets where records are kept;
☐	☐	☐	• Not sharing or openly posting employee passwords in work areas;
☐	☐	☐	• Encrypting sensitive customer information when it is transmitted electronically via public networks;
☐	☐	☐	• Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data; and
☐	☐	☐	• Reporting suspicious attempts to obtain customer information to designated personnel.
☐	☐	☐	Regularly remind all employees of your company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
☐	☐	☐	Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
☐	☐	☐	Impose disciplinary measures for security policy violations.
☐	☐	☐	Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.
☐	☐	☐	(***IRS suggestion:*** Add labels to documents to signify importance, such as "Sensitive" or "For Official Business" to further secure paper documents.)

Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Here are some FTC suggestions on maintaining security throughout the life cycle of customer information, from data entry to data disposal.

Ongoing	Done	N/A	
			Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
☐	☐	☐	Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.
☐	☐	☐	Store records in a room or cabinet that is locked when unattended.
☐	☐	☐	When customer information is stored on a server or other computer, ensure that the computer is accessible only with a "strong" password and is kept in a physically secure area.
☐	☐	☐	Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
☐	☐	☐	Maintain secure backup records and keep archived data secure by storing it offline and in a physically secure area.
☐	☐	☐	Maintain a careful inventory of your company's computers and any other equipment on which customer information may be stored.
			Take steps to ensure the secure transmission of customer information. For example:
☐	☐	☐	When you transmit credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit. (**IRS Suggestion:** Transport Layer Security 1.1 or 1.2 is newer and more secure.)
☐	☐	☐	If you collect information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
☐	☐	☐	If you must transmit sensitive data by email over the Internet, be sure to encrypt the data.

Ongoing	Done	N/A	
			Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule. For example:
☐	☐	☐	Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
☐	☐	☐	Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
☐	☐	☐	Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or other electronic media or hardware containing customer information.

Detecting and Managing System Failures

Effective security management requires your company to deter, detect, and defend against security breaches. That means taking reasonable steps to prevent attacks, quickly diagnosing a security incident, and having a plan in place for responding effectively. Consider implementing the following procedures:

Ongoing	Done	N/A	
☐	☐	☐	Monitor the websites of your software vendors and read relevant industry publications for news about emerging threats and available defenses.
			Maintain up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:
☐	☐	☐	• Check with software vendors regularly to get and install patches that resolve software vulnerabilities;
☐	☐	☐	• Use anti-virus and anti-spyware software that updates automatically;
☐	☐	☐	• Maintain up-to-date firewalls, particularly if you use a broadband Internet connection or allow employees to connect to your network from home or other off-site locations;
☐	☐	☐	• Regularly ensure that ports not used for your business are closed; and
☐	☐	☐	• Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

Ongoing	Done	N/A	
			Use appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It is wise to:
☐	☐	☐	• Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;
☐	☐	☐	• Use an up-to-date intrusion detection system to alert you of attacks;
☐	☐	☐	• Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
☐	☐	☐	• Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges
			Take steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
☐	☐	☐	• Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
☐	☐	☐	• Preserve and review files or programs that may reveal how the breach occurred; and
☐	☐	☐	• If feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.
			Consider notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
☐	☐	☐	• Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
☐	☐	☐	• Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
☐	☐	☐	• Notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business; and
☐	☐	☐	• Check to see if breach notification is required under applicable state laws.
☐	☐	☐	• (***IRS suggestions***: Practitioners who experience a data loss should contact the IRS and the states. Also, consider having a technical support contract in place, so that hardware events can be fixed within a reasonable time and with minimal disruption to business availability.)