



**Written Information Security Plan for
PAXUS CPA**

Table of Contents

1. Purpose and Scope of the Written Information Security Program3

2. Program Ownership and Responsibility3

3. Risk Assessment and Management4

4. Design and Implement Safeguards to Control Risks4

5. Employee Security Awareness:7

6. Service Provider Risk Management8

7. Program Evaluation and Updates8

8. Written Incident Response Plan.....8

9. Annual Review Process8

Disclaimer:

This *Written Information Security Plan* and the accompany documents *Written Incident Response Plan* and *Risk Assessment Matrix* are provided by Practice Protect for informational purposes only and is intended to serve as a general guide to help organizations understand the principles and best practices related to information security. While every effort has been made to ensure the accuracy and relevance of the information contained in this Plan, it is essential to recognize that each organization's unique circumstances, operations, and regulatory requirements may vary.

Customization and Review:

We strongly recommend that organizations carefully review and customize this Plan to suit their specific needs, risks, and compliance obligations, especially in relation to the Federal Trade Commission's (FTC) Safeguards Rule. The Plan's contents should be tailored to align with your organization's policies, procedures, and operational practices.

Legal Compliance:

It is crucial for organizations to seek legal counsel or consult with qualified professionals to ensure that their information security measures, policies, and practices comply with all applicable laws, regulations, and industry standards, including the FTC Safeguards Rule.

Limitation of Liability:

Practice Protect assumes no liability or responsibility for any actions taken or decisions made by organizations based on the information provided in this Plan. Use of this Plan is at your own discretion and risk.

By downloading and using this Plan, you acknowledge and agree to the above terms. Practice Protect disclaims any warranties or guarantees, expressed or implied, regarding the accuracy, completeness, or suitability of the information contained herein.



1. Purpose and Scope of the Written Information Security Program

The purpose of this Information Security Program is to establish a comprehensive framework to safeguard nonpublic personal information (NPI) and ensure compliance with the Federal Trade Commission's (FTC) Safeguards Rule. This program outlines the policies, procedures, and controls that **PAXUS CPA** will implement to mitigate risks, protect customer data, and maintain the confidentiality and integrity of sensitive information.

The scope of this program encompasses all aspects of **PAXUS CPA's** operations involving the collection, processing, storage, and transmission of NPI. It applies to all employees, contractors, and third-party service providers who have access to NPI or are involved in the management of data security within our organization. By establishing this program, we demonstrate our commitment to maintaining the highest standards of data security and privacy in line with regulatory requirements.

1.1 Overview of the FTC Safeguards Rule and Its Significance

The FTC Safeguards Rule, enacted under the Gramm-Leach-Bliley Act, is a crucial regulatory framework designed to protect consumer information and enhance data security practices within financial institutions. The rule mandates that organizations develop and maintain comprehensive information security programs to safeguard nonpublic personal information from unauthorized access, breaches, and other security incidents.

Under the FTC Safeguards Rule, financial institutions are required to identify and assess potential risks associated with NPI handling, implement appropriate safeguards, and establish incident response and breach notification procedures. Compliance with the Safeguards Rule not only ensures the protection of customer data but also reinforces trust between our organization and our clients.

By implementing an effective Information Security Program aligned with the FTC Safeguards Rule, **PAXUS CPA** not only meet regulatory obligations but also demonstrate our dedication to data privacy, security, and maintaining the confidentiality of the information entrusted to us.

2. Program Ownership and Responsibility

2.1 Designation of Individuals Responsible for the Program's Oversight and Implementation

The successful implementation and oversight of our Information Security Program require dedicated leadership and coordination. The following individuals have been designated with specific responsibilities for ensuring the effectiveness of the program:

LISA DIONISIO: As the **OWNER**, **LISA DIONISIO** will serve as the program owner and overall responsible party for overseeing the development, implementation, and ongoing management of the Information Security Program. **LISA DIONISIO** will collaborate with key stakeholders to ensure that the program aligns with business objectives and regulatory requirements.

2.2 Roles and Responsibilities of Key Personnel Involved in Maintaining Data Security

In addition to the program owner, several key personnel contribute to the maintenance and enforcement of data security measures within our organization:

Jennifer Sanders – Firm Administrator

PAXUS CPA uses Practice Protect as our cybersecurity provider. clientsuccess@practiceprotect.com is Practice Protect's primary contact department.



These individuals collaborate closely to ensure that the policies, procedures, and controls outlined in the Information Security Program are effectively communicated, enforced, and updated as needed. They are committed to upholding the confidentiality, integrity, and availability of nonpublic personal information and fostering a culture of data security within our organization.

3. Risk Assessment and Management

3.1 Description of the Risk Assessment Process to Identify Threats and Vulnerabilities

Our risk assessment process is designed to systematically identify and evaluate potential threats and vulnerabilities that could compromise the security and confidentiality of nonpublic personal information (NPI). This process involves:

Identification of internal and external threats that could lead to unauthorized access, breaches, or misuse of NPI.

Assessment of vulnerabilities within our systems, networks, processes, and third-party relationships that may be exploited by threats.

Evaluation of the potential impact of security incidents on the confidentiality, integrity, and availability of NPI.

3.2 Methodology for Assessing Risks, Including Likelihood and Potential Impact

To assess risks, we employ a structured methodology that involves quantifying the likelihood and potential impact of each identified threat-vulnerability pair. Likelihood is determined based on historical incidents, industry trends, and the cybersecurity landscape, while potential impact is evaluated considering financial, reputational, legal, and operational consequences.

The likelihood and impact are categorized into predefined levels, allowing us to assign a risk score to each pair. This scoring enables us to prioritize risks effectively and allocate resources where they are most needed.

3.3 Procedures for Prioritizing Risks and Implementing Appropriate Safeguards

Once risks are assessed and scored, we prioritize them based on their risk scores, potential impact, and other contextual factors. High-priority risks are addressed first, followed by medium and low-priority risks.

For each identified risk, we develop and implement appropriate safeguards, controls, and mitigation strategies. These safeguards may include but are not limited to encryption, access controls, regular security assessments, security awareness training, and incident response plans. The effectiveness of implemented safeguards is continuously monitored, and adjustments are made as needed to maintain a strong security posture.

3.4 Risk Assessment Table

See "*Risk Assessment Matrix*" Document

4. Design and Implement Safeguards to Control Risks

This section outlines our proactive approach to controlling risks identified through our comprehensive risk assessment process, in accordance with the FTC Safeguards Rule. Through these safeguards, we aim to uphold the confidentiality and integrity of nonpublic personal information (NPI), ensuring compliance and fostering trust with our clients.



4.1 Internal Applications

PAXUS CPA uses Practice Protect Access Hub as our Access Management system for Internal Applications. Some of the core features of this are:

<p>Centralized Access Management From banking to tax logins, our employees and contract workers have one login to access every internal application securely.</p>	<p>Managed Multi-Factor Authentication MFA is managed and enforced for all team members and contract workers through Practice Protect.</p>	<p>Advanced User & Team Permissions Roles and permissions are used to easily determine the level of access employees and contract workers have.</p>
<p>IP-Lock + Time-Lock + Location-Lock We implement controls on where, when, & what devices employees and contract workers can access certain applications on.</p>	<p>Passwordless Authentication Passwords are used by team members and contract workers but never seen, passwords are shared but encrypted and kept secure.</p>	<p>One-Click User Lockout We can revoke access instantly for team member offboarding or threat responses.</p>
<p>Remote & Third-Party Access Controls Remote team and contractor access is controlled through Practice Protect.</p>	<p>User Activity Tracking Using Practice Protect we can track and report on every login session & application access history with user, device, location & time stamps.</p>	

4.2 Client Applications

PAXUS CPA uses Practice Protect Access Hub as our Access Management system for Client Applications. Some of the core features of this are:

<p>Centralized Access Management From banking to tax logins, our employees and contract workers have one login to access every internal application securely.</p>	<p>Managed Multi-Factor Authentication MFA is managed and enforced for all team members and contract workers through Practice Protect.</p>	<p>Advanced User & Team Permissions Roles and permissions are used to easily determine the level of access employees and contract workers have.</p>
<p>IP-Lock + Time-Lock + Location-Lock We implement controls on where, when, & what devices employees and contract workers can access certain applications on.</p>	<p>Passwordless Authentication Passwords are used by team members and contract workers but never seen, passwords are shared but encrypted and kept secure.</p>	<p>One-Click User Lockout We can revoke access instantly for team member offboarding or threat responses.</p>
<p>Remote & Third-Party Access Controls</p>	<p>User Activity Tracking</p>	



Remote team and contractor access is controlled through Practice Protect.

Using Practice Protect we can track and report on every login session & application access history with user, device, location & time stamps.

4.3 File Storage & Sharing

PAXUS CPA uses Practice Protect Access and Device Hub as part of our data encryption program.

Passwordless Authentication

Passwords are used by team members and contract workers but never seen, passwords are shared but encrypted and kept secure.

IP-Lock + Time-Lock + Location-Lock

We implement controls on where, when, & what devices employees and contract workers can access certain applications on.

User Activity Tracking

Using Practice Protect we can track and report on every login session & application access history with user, device, location & time stamps.

Secure Information & File Storage

Sensitive information is stored & shared internally as an encrypted note or attachment using Practice Protect Secured Items.

Next Level Ransomware Protection

Unknown programs & files are opened in a secure location to safeguard existing data.

4.4 Email System

PAXUS CPA uses Practice Protect Email hub is used to protect our workstations and local applications. Some of the core features are:

Passwordless Authentication

Passwords are used by team members and contract workers but never seen, passwords are shared but encrypted and kept secure.

User Activity Tracking

Using Practice Protect we can track and report on every login session & application access history with user, device, location & time stamps.

IP-Lock + Time-Lock + Location-Lock

We implement controls on where, when, & what devices employees and contract workers can access certain applications on.

Advanced Spam Filter

Practice Protect has deployed customized spam filters to scan and quarantine suspicious emails before they are received.

Managed Email System Support

Practice Protect proactively manages our email system to ensure all changes are carried out in a secure method & conduct investigations into suspicious emails.



4.5 Company Devices

PAXUS CPA uses Practice Protect Device Hub to protect our workstations and local applications. Some of the core features are:

<p>Next Level Ransomware Protection Unknown programs & files are opened in a secure location to safeguard existing data.</p>	<p>AI Powered Threat Detection System Antivirus powered by Artificial intelligence is used to identify and prevent potential security threats including zero-day threats.</p>
<p>Managed desktop security & antivirus Advanced antivirus managed and updated by a team of cybersecurity professionals</p>	<p>Virtual Firewall Advanced virtual barrier around your firm’s computers, preventing unauthorized access from outside sources.</p>

4.6 Customer Information Disposal and Retention

PAXUS CPA uses Practice Protect to control employee access to customer information. When employees leave the firm, we revoke all access to the system, ensuring that only appropriate team members have access to customer information.

4.7 Change Management Procedures

PAXUS CPA has Practice Protect as our primary cyber security supplier. All major changes to our cybersecurity are managed and deployed in line with Practice Protect support protocols as outlined in the proposal agreement we signed with them.

5. Employee Security Awareness:

We recognize that a strong culture of security awareness is pivotal in maintaining the integrity of our information security practices and complying with the Federal Trade Commission's (FTC) Safeguards Rule. This section outlines our approach to educating employees and stakeholders about data security, privacy best practices, and their roles in protecting nonpublic personal information (NPI).

5.1 Security Awareness Programs:

We are committed to fostering a culture of data security awareness across our organization. Regular security awareness programs will be designed and conducted to educate employees and stakeholders about the risks associated with handling NPI. These programs will cover topics such as phishing awareness, social engineering, secure data handling, password management, and the importance of reporting security incidents promptly.

PAXUS CPA has Practice Protect as our primary cyber security supplier. All of our employees have access to Practice Protect University which has a library of over 18 hours of cybersecurity training and is updated regularly.

5.2 Training Initiatives:

Training initiatives will be tailored to the roles and responsibilities of employees and stakeholders. New hires will receive comprehensive training on data security practices during their orientation. Ongoing training sessions will be conducted to address emerging threats and regulatory updates. Training content will emphasize the importance of compliance with our Information Security Program and the FTC Safeguards Rule.



5.3 Incident Response Training:

Employees will be educated about our incident response procedures, ensuring they understand their roles in promptly reporting and responding to security incidents. Simulated exercises and tabletop drills will be conducted periodically to test the effectiveness of our incident response plans.

5.3.1 In addition, a security event affecting 500 or more people must be reported to the Federal Trade Commission (FTC) as soon as possible, but no later than 30 days after the date of discovery. This is in addition to reporting the incident to an IRS stakeholder liaison and state tax authorities.

5.4 Continuous Improvement:

We are committed to continuously improving our security awareness and training initiatives. Feedback from employees and stakeholders will be sought to refine training content, delivery methods, and program effectiveness.

6. Service Provider Risk Management

6.1 Evaluation of Third-Party Vendors' Security Practices:

We recognize that third-party relationships can pose potential risks to the security of nonpublic personal information (NPI) in our custody. Therefore, we have established a robust third-party risk management process to evaluate the security practices of vendors before engaging their services.

Our Key third Party Service Providers are below with links to information on their security practices:

1. Practice Protect - <https://practiceprotect.com/accreditations/>
2. KnowBe4 - <https://www.knowbe4.com/about-us>
3. Financial Cents - <https://financial-cents.com/security/>
4. QuickBooks Online - <https://security.intuit.com/security-practices/>

7. Program Evaluation and Updates

We are committed to maintaining the effectiveness and relevance of our information security program in alignment with the Federal Trade Commission's (FTC) Safeguards Rule. We understand that periodic evaluation and adjustments are essential for its continued robustness. We will evaluate and update our information security program by considering the outcomes of required testing and monitoring (as specified in paragraph (d)), significant changes to our operations or business arrangements, the results of risk assessments performed according to paragraph (b)(2), and any other circumstances that may materially impact our information security program. Through this ongoing evaluation and proactive adaptation, we ensure that our information security measures remain resilient and compliant with regulatory mandates.

This plan was reviewed on the following:

- Implemented: **14 November 2024**

8. Written Incident Response Plan

We maintain a written incident response plan – see “*Written Incident Response Plan*” document.

9. Annual Review Process

We are committed to the ongoing effectiveness and relevance of our Information Security Program. The program will be subjected to periodic reviews to ensure alignment with the Federal Trade Commission's (FTC) Safeguards Rule,



technological advancements, evolving regulatory requirements, and changes in our business operations. These reviews will occur at least annually to assess the currency of our security measures.

9.1 Process for Incorporating Changes:

Our process for incorporating changes into the Information Security Program is designed to maintain its responsiveness to a dynamic environment. Changes may arise from emerging threats, regulatory modifications, technological enhancements, or shifts in our business practices. This process involves:

- **Identification:** Regular monitoring of industry trends, regulatory updates, and technological advancements to identify potential changes required.
- **Assessment:** Evaluating the impact of proposed changes on the effectiveness of our security measures and the alignment with the FTC Safeguards Rule.
- **Approval:** Securing approval from relevant stakeholders, including our information security team and senior management.
- **Communication:** Communicating changes to all employees and stakeholders, ensuring awareness and understanding of the updates.
- **Implementation:** Executing the necessary changes as per the approved plan, which may involve adjusting policies, procedures, controls, and training materials.

By adhering to this review and update process, we demonstrate our commitment to maintaining a robust Information Security Program that is both compliant with regulatory mandates and adaptive to the evolving landscape of security threats.

This plan was reviewed on the following:

- **Implemented: 14 November 2024**

