2023

FTC SAFEGUARDS

Rule Policies & Plans

Accountant Compliance

Made Easy:

Step By Step Checklist

Template & Guide Created by
Tech 4 Accountants
tech4accountants.net/ftc

FTC Safeguards

Rule Policies & Plan

For assistance with compliance go to **https://tech4accountants.net/FTC**
Template Created by Tech 4 Accountants

§ 314.5 Effective Date

Sections 314.4(a), (b)(1), (c)(1) through (8), (d)(2), (e), (f)(3), (h), and (i) are effective as of June 9, 2023. - FTC.gov

Last Audit

_____

Guide Created By:

Tech 4 Accountants

Safeguards Technology Provider

Extra Support & Guidance https://www.tech4accountants.net/ftc

All of the [below] elements outlined in the Safeguards Rule are relevant to help protect the security of customer information and are worthy of consideration by all sizes of CPA firms, regardless of the number of consumers for which customer information is maintained.

– Journal of Accountancy - February 1, 2023

TABLE OF CONTENTS

YOUR PERSONAL INFORMATION

First

Last

Company Name

Street Address 1

Street Address 2

City

State

Zip

Vendor / Person Conducting Report

PREREQUISITES

Introduction

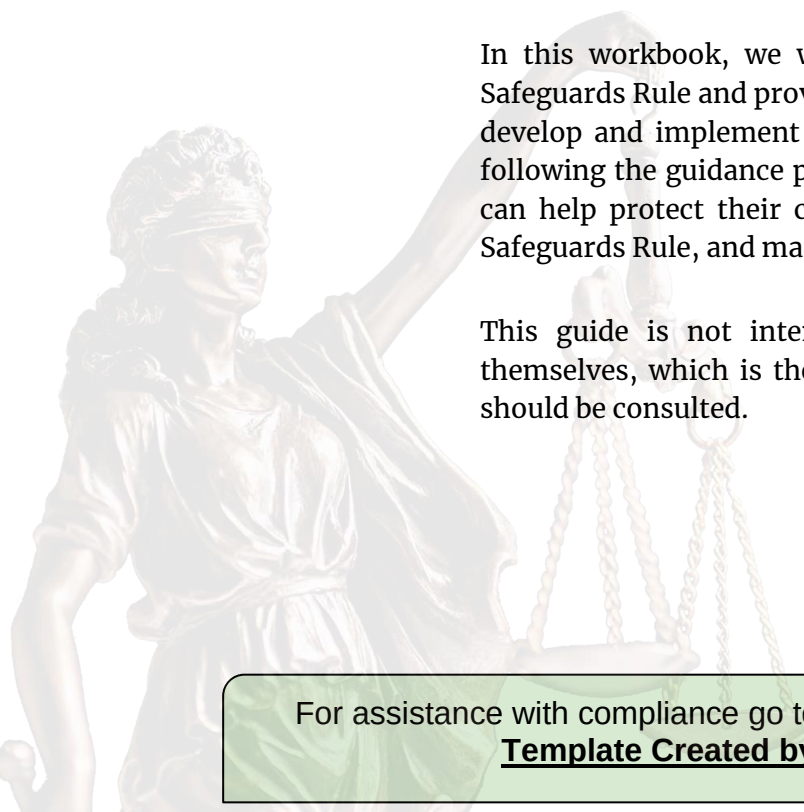
The Federal Trade Commission (FTC) Safeguards Rule is a set of regulations designed to protect the confidentiality and security of consumers' personal information. The Safeguards Rule requires certain financial institutions to develop, implement, and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards.

The FTC Safeguards Rule applies to accountants who handle sensitive financial information from their clients'. This includes accountants, bookkeepers, banks, credit unions, tax accountants, and other entities that offer financial products and services to consumers. These institutions are required to take reasonable steps to safeguard consumers' personal information from unauthorized access, use, or disclosure. The Safeguards Rule also requires these institutions to regularly monitor and assess the effectiveness of their information security programs.

The Safeguards Rule was enacted in response to the increasing use of electronic transactions and the growing risk of identity theft and other forms of fraud. The rule provides a framework for financial institutions to protect their clients' personal information and maintain their trust.

In this workbook, we will explore the key requirements of the FTC Safeguards Rule and provide templates and guidance to help accountants develop and implement an effective information security program. By following the guidance provided in this workbook, financial institutions can help protect their clients' personal information, comply with the Safeguards Rule, and maintain the trust of their clients'.

This guide is not intended to be a substitute for the FTC’s rules themselves, which is the definitive source and in all cases control and should be consulted.



Overview of Cybersecurity

Cybersecurity refers to the practice of protecting computer systems, networks, and digital information from unauthorized access, theft, damage, or other forms of unauthorized interference. Cybersecurity involves the use of various technologies, processes, and policies to prevent, detect, and respond to security threats and incidents.

For accountants, cybersecurity is particularly important as they handle sensitive personal information of their clients, such as names, addresses, social security numbers, and financial information. Cybercriminals and hackers target accountants as a prime source of valuable personal data. A successful data breach can result in significant financial losses, legal liabilities, and reputational damage for the affected business.

A comprehensive cybersecurity program can help protect a business against cyber threats by implementing safeguards to prevent unauthorized access, detecting security breaches, and responding quickly to mitigate damage. The FTC Safeguards Rule requires accountants to implement an information security program that is designed to protect client data, including administrative, technical, and physical safeguards. By complying with the Safeguards Rule, businesses can better protect their clients' personal information and reduce the risk of financial losses, legal liabilities, and reputational damage.

Checklist: Required FTC Software

	Description	Citation	Pass/Fail	Vendor/Date
☐	Hire Qualified Individual / Service Provider	16 CFR 314.4(a)		
☐	Conduct Risk Assessment	16 CFR 314.4(a)		
☐	Encryption At Rest	16 CFR 314.4 (c) (3)		
☐	Encryption in Transit	16 CFR 314.4 (c) (3)		
☐	Multi Factor Authentication	16 CFR 314.4 (c) (5)		
☐	Continuous Monitoring with IDS / RMM or Network Scan & Penetration Testing	16 CFR 314.4 (d) (2)		
☐	Security Awareness Training	16 CFR 314.4 (e)		
☐	Date: Assess Providers	16 CFR 314.4 (f)		
☐	Date: Annual WISP Review	16 CFR 314.4 (g)		
☐	Develop an Incident Response Plan	16 CFR 314.4 (h)		
☐	Date: Annual Director Reports	16 CFR 314.4 (h)		
☐	Date: Annual Disposal of Records	FTC SWS (1)		
☐	Restricted Access to Data	FTC SWS (2)		
☐	Require Complex Passwords	FTC SWS (3)		
☐	Firewall	FTC SWS (5)		
☐	Intrusion Detection Systems (IDS)	FTC SWS (5)		
☐	Segmented / IOT / Guest Network	FTC SWS (5)		
☐	Endpoint Security	FTC SWS (6)		
☐	3rd Party Patch Management	FTC SWS (6)		
☐	Windows Patch Management	FTC SWS (6)		

For assistance with compliance go to **https://tech4accountants.net/FTC**
Template Created by Tech 4 Accountants

FTC Start with Security (SWS): A Guide for Business

1. **Start with Security**
    a. Don't collect personal information you don't need
    b. Hold on to information only as long as you have a legitimate need
    c. Don't use personal information when it's not necessary
2. **Control Access to Data Sensibly**
    a. Restrict access to sensitive data
    b. Limit administrative access
3. **Require Secure Passwords and Authentication**
    a. Insist on complex and unique passwords
    b. Store passwords securely
    c. Guard against brute force attacks
    d. Protect against authentication bypass
4. **Store Sensitive Information Securely & Protect It During Transmission**
    a. Keep sensitive information secure throughout its lifecycle
    b. Use industry-tested and accepted methods
    c. Ensure proper configuration
5. **Segment Your Network and Monitor Who's Trying To Get In & Out**
    a. Segmented IOT network
    b. Segment Guest Network
6. **Secure Remote Access to Your Network**
    a. Ensure endpoint security is installed
    b. Put sensible access limits in place
7. **Apply Sound Security Practices When Developing New Products**
    a. Train your engineers in secure coding
    b. Follow platform guidelines for security
    c. Verify that privacy features work
8. **Ensure Service Providers Implement Reasonable Security Measures**
    a. Put in writing and verify compliance
9. **Create Procedures to Address Issues That May Arise**
    a. Update and patch third-party software
    b. Heed credible security warnings and move quickly to fix them
10. **Secure paper, physical media, and devices**
    a. Securely store sensitive files
    b. Protect devices that process personal information
    c. Keep safety standards in place when data is in route

REQUIREMENT 1

Designate a Qualified Individual To Oversee Security Program § 314.4

Requirement

Designate a qualified individual to implement and supervise your company's information security program, in accordance with 16 CFR 314

Who is your Qualified Service Provider / Individual?

- _____

What makes them qualified to be able to oversee your security program?

- _____
- _____
- _____

List examples of their real-world experience overseeing security programs:

- _____
- _____
- _____

How are you supervising their performance?

- _____
- _____
- _____

Do you take responsibility for their compliance? Yes (Required) / No

Do they have an ISP that protects your firm? Yes (Required) / No

REQUIREMENT 2

Develop a Written Risk Assessment

Requirement Outcome

While acknowledging there will be some cost to conducting a risk assessment, the Commission believes a properly conducted risk assessment is an essential part of a financial institution's information security program. The entire Safeguards Rule, both as it currently exists and as amended, requires that the information security program be based on a risk assessment. - https://www.federalregister.gov/

Who will be responsible for performing the risk assessment?

- _____

What criterial will be used for evaluating and categorizing security risks?

- _____
- _____
- _____
- _____
- _____
- _____
- _____

Assess the adequacy of existing systems in terms of:

- **Confidentiality**
  - _____
- **Integrity**
  - _____
- **Information Availability**
  - _____
- **How will identified risks be mitigated or accepted and how will they be addressed?**
  - _____
  - _____
  - _____
  - _____
- **How will you evaluate and adjust your plan in light of result & material changes?**
  - _____
  - _____
  - _____
  - _____
  - _____
  - _____

Types of Information Collected

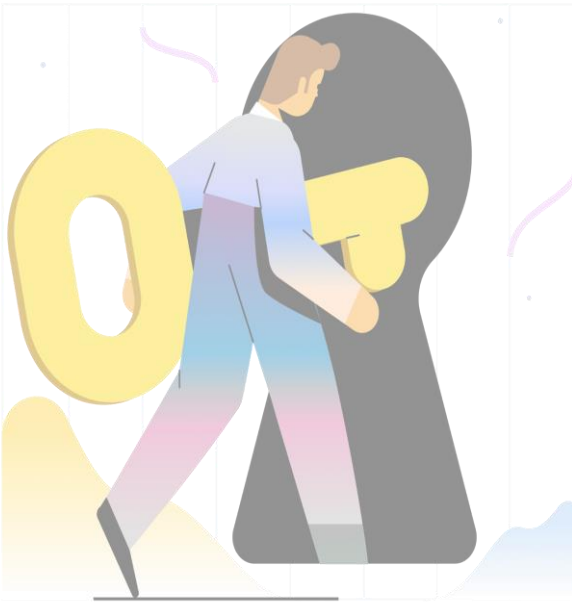
- Social Security Numbers of the taxpayer and their dependents
- Dates of birth of the taxpayer and their dependents
- Wages and salary information
- Investment income and gains/losses
- Information related to rental properties and real estate investments
- Bank account and routing numbers for direct deposit of refunds or payments
- Credit card and loan information
- Business income and expense information
- Contact information not publicly available like email and phone numbers
- Health care information for tax credits and deductions
- List of business client's customer list and their information

Risk Assessment (Based on AICPA SOC2 Framework)

1. Define Your Business Objectives

- **Security:** Protect the confidentiality, integrity, and availability of both our own, and our clients' data through implementation of appropriate security controls and measures.
- **Availability:** Ensure that our systems and services are available to our clients as needed by minimizing the risk of unplanned downtime and implementing appropriate disaster recovery and business continuity plans.
- **Processing Integrity:** Process transactions accurately and completely in accordance with our clients' expectations and industry standards, by implementing appropriate controls and measures.
- **Confidentiality:** Maintain the confidentiality of our own and our clients data by ensuring that access to this data is restricted to authorized personnel only, and by implementing appropriate encryption and access controls.
- **Privacy:** Protect the privacy of our own and our clients' data by implementing appropriate privacy policies and procedures which must comply with privacy laws.

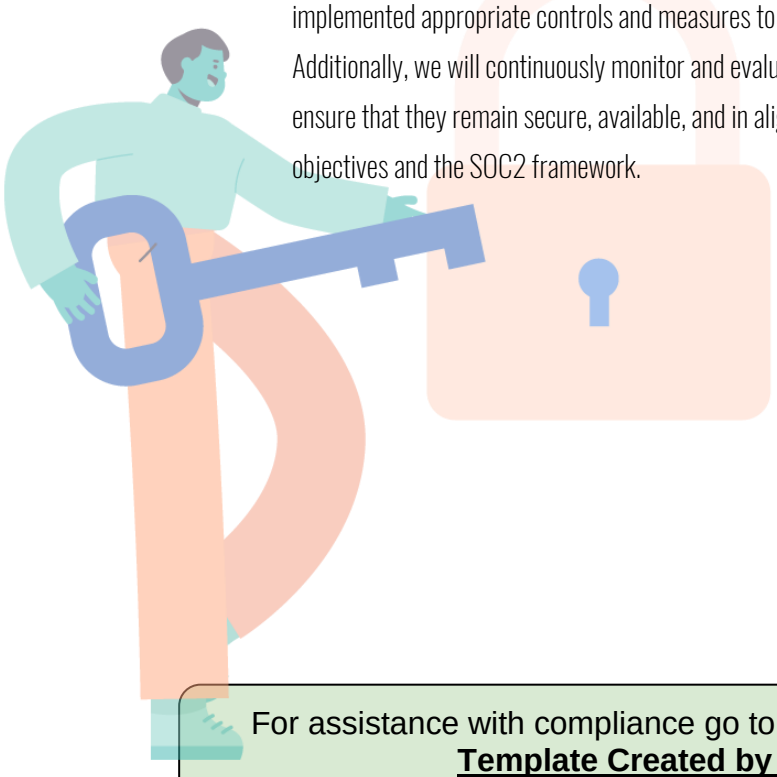
These business objectives will guide our organization in implementing appropriate controls and measures to achieve SOC2 compliance and in continuously monitoring and improving our security, availability, processing integrity, confidentiality, and privacy practices. By following SOC2 guidelines, We will demonstrate our commitment to the security, availability, processing integrity, confidentiality, and privacy of our clients data and our own data, and provide assurance to our clients and stakeholders that we have implemented appropriate controls and measures to protect their information. This workbook uses SOC 2 as a framework, and does not constitute actual SOC 2 Compliance.



2. Identify In-Scope Systems

- **Customer Management System:** This system is used to manage customer information including personal information and financial data. The system is used by authorized personnel to input, access, and manage customer data.
- **Financial Management System:** This system is used to manage financial data including billing, accounts receivable, and accounts payable. The system is used by authorized personnel to input, access, and manage financial data.
- **Human Resources Management System:** This system is used to manage employee data including personal information and payroll data. The system is used by authorized personnel to input, access, and manage employee data.
- **IT Infrastructure:** This includes all hardware and software components used to support our business operations including servers, network devices, and cloud services. It is used to host and process financial, client and employee data.

These in-scope systems will be subject to our SOC2 audit and will be evaluated against the applicable Trust Services Criteria. By identifying our in-scope systems, we can ensure that we are focusing our SOC2 efforts on the most critical systems and data, and can provide assurance to our clients and stakeholders that we have implemented appropriate controls and measures to protect their information. Additionally, we will continuously monitor and evaluate our in-scope systems to ensure that they remain secure, available, and in alignment with our business objectives and the SOC2 framework.



3. Perform Risk Analysis

The following risk analysis has been performed to identify potential risks to the confidentiality, integrity, and availability of our clients' data, as well as our own data:

4. Document Risk Responses

	RESPONSES
RISK **Unauthorized access to customer data.** *This could result in the exposure of sensitive information, loss of data, and damage to the company's reputation.*	*To mitigate the risk of unauthorized access to customer data, the company will implement strong access controls, such as password policies, multi-factor authentication, and role-based access. In addition, regular security training will be provided to all employees to ensure they are aware of the risks and the proper security procedures.*
RISK **Network outage or system failure.** *This could result in downtime for critical systems, loss of revenue, and damage to the company's reputation.*	*To mitigate the risk of network outages or system failures, the company will implement a redundant network architecture, backup and disaster recovery procedures, and regular testing of these procedures to ensure they are effective. In addition, the company will maintain a service level agreement (SLA) with its customers, which includes guarantees for uptime and availability.*
RISK **Inadequate physical security.** *This could result in the theft of hardware, loss of data, and damage to the company's reputation.*	*To mitigate the risk of inadequate physical security, the company will implement strict access controls to its data centers and offices, including biometric identification and surveillance systems. In addition, all hardware will be secured with locks and alarms to prevent theft or unauthorized access.*
RISK **Human error or malicious behavior.** *This could result in the accidental or intentional deletion, modification, or disclosure of sensitive data.*	*To mitigate the risk of human error or malicious behavior, the company will implement strict access controls, regular security training for all employees, and monitoring and logging of all user activity. In addition, the company will conduct regular security audits and penetration testing to identify and address vulnerabilities in its systems.*

Checklist: Data Storage

List anywhere that contains PII. Examples include but are not limited to:

1. Tax Software(s)
   a. _____
   b. _____
2. Bookkeeping Software(s)
   a. _____
   b. _____
3. Payroll Software(s)
   a. _____
   b. _____
4. 3rd Party Apps
   a. _____
   b. _____
5. Cloud Provider(s)
   a. _____
   b. _____
6. Data Storage(s)
   a. _____
   b. _____
7. Email Provider(s)
   a. _____
   b. _____
8. CRM(s)
   a. _____
   b. _____
9. Social Media Contractor(s)
   a. _____
   b. _____

Employee / Contractor: Data Storage

Employee / Contractor Name	Computer Name Holding PII
<Example John Smith>	<Example DESKTOP-ABCDEF>

Policy & Procedure to Assess Contractors / Vendors / Software Providers

➢ Introduction

Our accounting firm relies on third-party contractors, vendors, and software providers to provide us with products and services that are essential to our business operations. However, the use of these third parties also introduces potential risks to our clients' data and our overall security posture. This risk assessment policy and procedure is designed to help us assess and manage the risks associated with our third-party relationships.

➢ Scope

This risk assessment policy and procedure applies to all third-party contractors, vendors, and software providers who have access to our clients' data or who provide us with products or services that are essential to our business operations.

➢ Risk Assessment Criteria

The following criteria will be used to assess the risks associated with our third-party relationships:

a. Sensitivity of Data: The sensitivity of the data that the third party will have access to or handle.
b. Business Impact: The potential impact on our business operations if the third party experiences an outage or other business interruption.
c. Security Posture: The third party's security posture and ability to protect our clients' data.
d. Compliance: The third party's compliance with all applicable regulations and standards, including but not limited to: FTC, GLBA, GDPR, and SOC 2.
e. Contractual Terms: The terms of the contract with the third party, including but not limited to: liability, indemnification, and termination.

➢ Risk Assessment Process

The following process will be used to assess the risks associated with our third-party relationships:

a. Identify Third Parties: We will identify all third-party contractors, vendors, and software providers who have access to our clients' data or who provide us with products or services that are essential to our business operations.
b. Gather Information: We will gather information about each third party, including but not limited to: the sensitivity of the data they will have access to or handle, their security posture, and their compliance with applicable regulations and standards.
c. Assess Risks: We will assess the risks associated with each third-party relationship based on the criteria outlined in this policy.
d. Mitigate Risks: We will work with each third party to mitigate any risks identified during the assessment process. This may include, but is not limited to: requiring them to implement additional security measures or renegotiating contractual terms.
e. Monitor Risks: We will monitor the risks associated with our third-party relationships on an ongoing basis to ensure that they continue to be mitigated effectively.
f. Reporting Incidents: Any incidents related to a third-party contractor, vendor, or software provider must be reported to the IT department as soon as possible. This includes incidents related to security, compliance, or contractual terms.
g. Compliance: Failure to comply with this risk assessment policy and procedure may result in disciplinary action, up to and including termination of employment.

➢ Conclusion

Our accounting firm recognizes the importance of assessing and managing the risks associated with our third-party relationships. By following this risk assessment policy and procedure, we can ensure that we work with third parties who meet our security and compliance requirements, and who are committed to maintaining the same level of security and compliance that we require.

Policy & Procedure to Handle Change in Management

- Introduction

  Our organization recognizes that change in management can have significant impacts on our operations, employees, and stakeholders. This policy and procedure is designed to ensure that any changes in management are handled in a transparent, fair, and orderly manner that minimizes disruption to our business and employees.

- Scope

  This policy and procedure applies to any change in management within our organization, including but not limited to: promotions, transfers, retirements, resignations, terminations, or any other circumstance that results in a change in management.

- Communication

  A clear communication plan will be developed and implemented to inform all employees and stakeholders of the upcoming changes in management. The communication plan will include:

  a. A timeline for the transition
  b. The names of the new managers or leaders
  c. The roles and responsibilities of the new managers or leaders
  d. The reasons for the change in management
  e. The impact of the change in management on employees and stakeholders
  f. Any necessary training or support for employee
  g. Succession Planning

     - Succession planning is critical to ensure a smooth transition in the event of a change in management. The following steps will be taken to ensure that succession planning is in place:

- The outgoing manager will work with the incoming manager to transfer knowledge and information about the role, responsibilities, and ongoing projects.
- A comprehensive job description for the new manager will be developed and communicated to all stakeholders.
- A review of the existing talent within the organization will be conducted to identify potential candidates for the management position.
- A training and development plan will be created for the new manager to ensure that they have the skills and knowledge necessary to succeed in their new role.

- Employee Support

  During times of change in management, it is important to provide support to employees to help them cope with any stress or anxiety that may arise. The following steps are taken to support employees:

  a. Regular communication and updates will be provided to employees regarding the change in management and how it impacts them.
  b. Opportunities for employees to provide feedback or ask questions will be provided.
  c. Counseling or other support services will be made available to employees who are experiencing difficulty adjusting to the change.

- Compliance

  All changes in management will be handled in compliance with all applicable laws, regulations, and company policies.

- Conclusion

  Our organization recognizes that change in management can be difficult, but by following this policy and procedure, we can ensure that any changes are handled in a transparent, fair, and orderly manner that minimizes disruption to our business and employees.

Date to re-assess contractors / vendors / software providers _____

CRITERIA FOR
SECURITY

Instructions: List vendors for compliance. If there are multiple, separate each one with a comma.

Software	Vendor / Method
Antivirus	
Anti-Phishing Toolbar	
Firewall	
Remote Monitoring & Management (RMM)	
Encryption At Rest	
Encryption in Transit	
Intrusion Detection Systems (IDS)	
VPN	
2 Factor Authentication	
Endpoint Detection Software	
Backup Software	
Windows Patch Management	
3rd Party Patch Management	

- If you do not have software to meet compliance requirements, consider going to tech4accountants.net/ftc to purchase compliant software for less than retail pricing.

CRITERIA FOR
CONFIDENTIALITY

1. Access Controls

- Implement access controls to limit access to confidential information to authorized personnel
- Use strong passwords and two-factor authentication to prevent unauthorized access
- Regularly review access privileges to ensure they are still necessary and appropriate
- Log all access attempts and regularly review logs for suspicious activity
- Train employees on proper use and protection of confidential information

2. Encryption

- Use encryption to protect sensitive data both in transit and at rest
- Encrypt all files and data containing confidential information
- Ensure that all email communications containing confidential information are encrypted
- Use secure communication channels such as VPNs to transmit data over public networks
- Train employees on proper use and management of encryption tools

3. Employee Training

- Provide regular training to employees on best practices for handling confidential information
- Train employees on how to identify and report suspicious activity
- Implement policies and procedures for handling confidential information
- Test employee knowledge of policies and procedures through regular assessments
- Encourage a culture of confidentiality and accountability within the organization
- Recognize those who effectively identify phishing threats

4. Physical Security

- Implement physical access controls to limit access to areas containing confidential information
- Use surveillance cameras and monitoring systems to deter and detect unauthorized access
- Secure all storage areas containing confidential information with locks or other measures
- Properly dispose of physical documents and media containing confidential information
- Train employees on proper physical security measures and enforce policies and procedures.

5. Incident Response

- Procedure for identifying breach
    a. Regular monitoring of systems for suspicious activity or unusual behavior
    b. Implementing intrusion detection systems and other security tools to detect threats
    c. Regularly reviewing logs and other records for signs of unauthorized access
    d. Training employees on how to identify and report potential incidents or breaches

- Upon identifying a potential incident or breach, assess the situation:
    a. Gathering information on the incident, including the type of data involved, the extent of the breach, and the potential impact on clients and employees
    b. Determining the cause of the incident, including whether it was the result of a cyber-attack, human error, or other factors
    c. Assess the potential impact on our operations, clients, and employees

- Reporting

  All incidents or potential breaches will be promptly reported to senior management who will then determine whether to notify external stakeholders such as regulatory bodies or clients, as required by law or company policy.

6. Procedure for containing breach

- Immediately disconnecting affected systems or networks from the internet or other external networks to prevent further damage or data loss
- Implementing additional security measures such as firewalls or access controls to prevent unauthorized access to sensitive data
- Identifying the individuals or parties affected by the breach and notifying them
- Conducting a thorough investigation to determine the root cause of the incident and identifying any additional security measures that may be necessary to prevent future incidents
- Updating incident response plans and procedures as needed

CRITERIA FOR

INTEGRITY

Back-Up Software / Process Used

Note: Storage platforms like Google Drive, SharePoint, and Dropbox are NOT backup, they are storage.

1. **Version Control Policy**

- ➢ Documents will be stored in a central location with access to authorized personnel only
- ➢ All changes to documents must be tracked and documented using a change log
- ➢ Whenever a new version of a document is created, it will be labeled with a unique version number and date automatically by the software
- ➢ All staff will be instructed to use the latest version of each document in all activities

2. **Audit Trails Policy**

- ➢ Our organization maintains audit trails to monitor all activities related to cyber security
- ➢ All audit trails will include sufficient detail to enable reconstruction of events, and will be retained for a period of no more than 2 years
- ➢ Access to audit trails will be restricted to authorized personnel and vendors, and will be regularly monitored for suspicious activity

3. **Access Control Policy**

- ➢ Only authorized personnel can access our systems and data
- ➢ Access will be granted on a need-to-know basis with permissions regularly reviewed
- ➢ Any unauthorized access attempts will be logged and investigated

CRITERIA FOR

EVALUATING RISKS & THREATS

LIKELIHOOD	*How likely is the risk or threat to occur, based on historical data, industry trends, or other factors?*
IMPACT	*What would be the consequences of the risk or threat, such as financial loss, reputational damage, or legal liability?*
VULNERABILITY	*How vulnerable are the systems or processes that could be affected by the risk or threat, and how easy would it be to exploit these vulnerabilities?*
SEVERITY	*What is the severity of the potential harm that could be caused by the risk or threat, and how would this harm be classified (e.g. minor, moderate, or major)?*
MITIGATION	*What measures are currently in place to mitigate the risk or threat, and how effective are these measures?*
DETECTION	*How easily could the risk or threat be detected, and what systems or processes are in place to monitor for potential incidents?*
RECOVERY	*How quickly could the organization recover from the risk or threat, and what resources or contingency plans are in place to support this recovery process?*

How can information be misused, altered, or destroyed?

- ➢ **Unauthorized access:** Information can be misused if someone gains access to it without authorization either through hacking, social engineering, or other means
- ➢ **Malware:** Malicious software can be used to alter or destroy information on a system or to exfiltrate sensitive data to unauthorized parties
- ➢ **Insider threats:** Employees or contractors with authorized access to information can misuse it for personal gain or to harm the organization
- ➢ **Physical theft:** Physical theft of devices or documents containing sensitive information can result in loss or exposure of this information.
- ➢ **Human error:** Accidental mistakes or omissions by employees can lead to unintentional alteration or destruction of information
- ➢ **Natural disasters:** Natural disasters such as floods, fires, or earthquakes can damage or destroy physical devices or systems containing information
- ➢ **Cyber attacks:** Deliberate cyber attacks such as denial of service attacks, ransomware, or phishing attempts can disrupt or compromise systems and data leading to loss, alteration, or destruction of information

When will your periodic reassessment be conducted?

- **Date:_____**

Physical Storage Potential Threats:

- ➢ Employees
- ➢ Clients
- ➢ Cleaners
- ➢ Landlords
- ➢ Visitors
- ➢ Burglary
- ➢ Trash Diving
- ➢ Mail Theft
- ➢ Lost/Misplaced

Events that will elicit a change/modification in ISP:

- New server
- New laws
- New ownership / management
- Expansion to new area
- Incidents affecting peers in the same industry
- New vendors or contractors in use with access to PII
- Customer concerns
- Suggestion from IT provider
- Audit uncovers severe vulnerability

User / Access Monitoring Policy

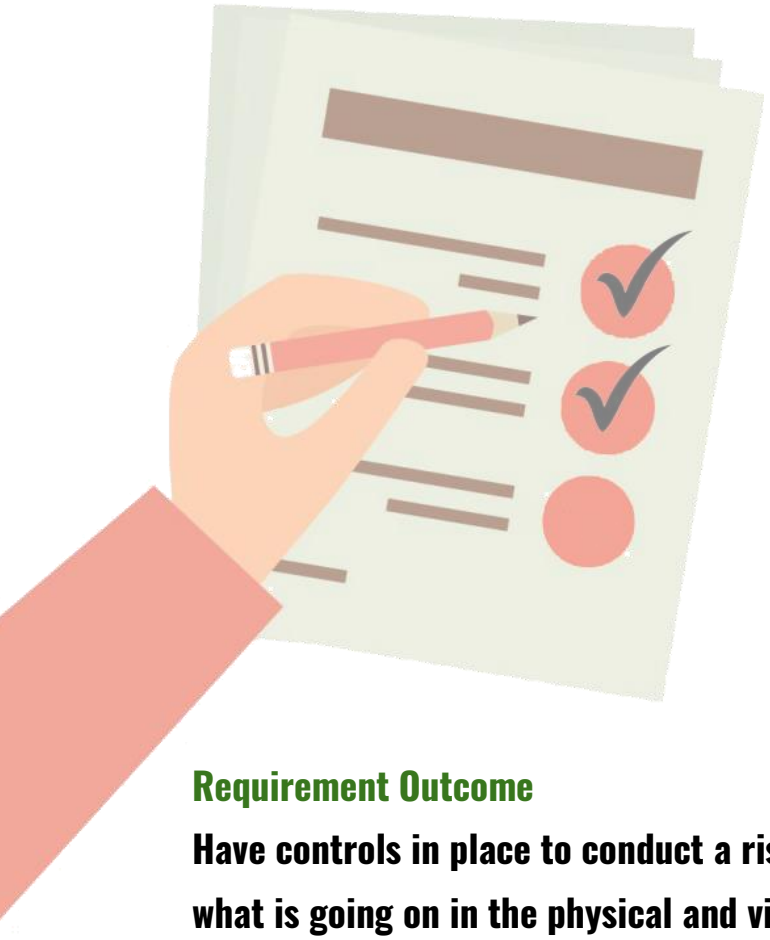
- We will implement access controls to ensure appropriate access to systems, applications, and data
- Monitor user activity and access using various tools and techniques on a regular basis, including reviewing logs and system alerts
- Personnel responsible for monitoring user activity and access will be trained to identify and respond to potential security threats or violations
- In the event of a security incident or violation reporting requirements, escalation procedures, and notification procedures will be followed.
- We will retain monitoring data for a defined period and dispose of it securely
- This policy applies to all personnel and end-users accessing our systems, applications, and data

What software is used to monitor?

Monitoring Software Name: _____

Who is the qualified individual to carry out the monitoring?

Qualified Individual Name: _____



REQUIREMENT 3

Design and Implement Controls Through Risk Assessment

Requirement Outcome

Have controls in place to conduct a risk assessment and know how to measure what is going on in the physical and virtual networks.

Frequency of Conducting Periodic Reviews: _____

→ Authenticate and Permit Access Policy for Authorized Users

1. **Policy Title**

   Secure Access Control: Implementing authentication and authorization policies for authorized users

2. **Policy Statement**

   The organization shall implement an authentication and authorization policy to ensure that only authorized users have access to its information systems and data. This policy applies to all employees, contractors, consultants, vendors, and other individuals who have access to the organization's information systems.

3. Purpose

The purpose of this policy is to ensure that only authorized users have access to the systems and data they need to perform their job functions.

4. Scope

This policy applies to all employees, contractors, vendors, and other third-party users who access company systems and data.

5. Access Control

Access to systems and data must be controlled based on the principle of least privilege. Only those who require access to perform their job functions should be granted access.

a. Authentication: This is the process of verifying the identity of a user or device. All users must be authenticated before being granted access to systems and data. This can be achieved through the use of passwords, biometric authentication, or other authentication methods.
b. Password Requirements: Passwords used by employees within the company must meet the following requirements:
c. At least 8 characters long
d. Contain at least one uppercase letter, one lowercase letter, one number, and one special character
e. Must be changed every 90 days
f. Cannot be reused for at least 10 password changes
g. Must not be written down or shared with others
h. Multi-factor Authentication: Multi-factor authentication (MFA) is the use of two or more authentication factors to verify the identity of a user. MFA must be used for all remote and privileged access
i. Access Monitoring: All access to systems and data must be logged and monitored. Any suspicious activity must be reported to the appropriate personnel for investigation.

6. Termination of Access: Access to systems and data must be terminated immediately upon an employee's termination, contract expiration, or other forms of separation from the company.
7. Review and Audit: Access to systems and data must be reviewed and audited periodically, ensuring access is still required.
8. Enforcement: Violation of this policy may result in disciplinary action, up to and including termination of employment or contract.

How you will limit authorized users access to need-to-know information?

1. **Access Control**

   The company will implement strict access control measures to ensure that only authorized personnel have access to sensitive information. This includes password protection, two-factor authentication, and limiting access to the need-to-know basis.

2. **Data Classification**

   The company will classify its data according to its sensitivity and the level of access that each employee is authorized to have. The levels of classification will include public, confidential, and highly confidential, and access will be granted only to employees who need it.

3. **Regular Review**

   The company will regularly review its access control policies and procedures to ensure that

they are up-to-date and effective. Any changes in employee responsibilities or job functions that require access to new information will be updated in the access control system.

4. **Training**

   All employees will receive regular training on the company's access control policies and procedures. This training will include information on the classification of data, the importance of protecting sensitive information, and the consequences of unauthorized access.

5. **Audit Trail**

   The company will maintain an audit trail of all access to sensitive information. This will include the date and time of access, the name of the user, and the data that was accessed. The audit trail will be regularly reviewed to identify any unauthorized access attempts.

6. **Termination Procedure**

   When an employee leaves the company, access to all sensitive information will be immediately revoked. This will include the deactivation of login credentials, removal of access rights, and any other necessary actions to ensure that the information is protected.

How to identify and manage data, personnel, devices, and facilities

1. **Identify Sensitive Data**

   It is essential to identify sensitive data, such as financial information, tax information, and personal information of clients, and categorize it based on its level of sensitivity.

2. **Implement Access Controls**

   Implement access controls to limit access to sensitive data. This could include implementing password policies, two-factor authentication, and role-based access controls.

3. **Perform Regular Risk Assessments**

   Regularly assess risks to data, personnel, devices, systems, and facilities to identify potential vulnerabilities and implement measures to mitigate them.

4. **Train Employees**

   Train employees on information security policies and procedures to ensure that they understand their role in safeguarding sensitive information.

5. **Use Secure Devices & Systems**

   Use secure devices and systems, such as encrypted laptops and servers, to protect data from unauthorized access.

6. **Implement Physical Security Measures**

   Implement physical security measures, such as restricted access to server rooms and secure document storage, to prevent unauthorized access to physical facilities.

Disposal of Customer Information Policy

GAAP Requirements for Accountants

TYPE OF DOCUMENT	RESPONSIBLE DEPARTMENT	RETENTION PERIOD
Account Reconciliations (Assets And Liabilities)	*Appropriate department*	**7 years**
Accounting Reports (Monthly Departmental Reports)	*Appropriate department*	**7 years / 3 years**
Accounts Payable Invoices, Check Requests, And Related Documents	*Appropriate department*	**7 years**
Actuarial Reports (Fasb Plans, Wc, Ltd, Health Plans)	*Appropriate department*	**Permanent**
Annual Gaap Financial Reports	*Financial Reporting*	**Permanent**
Banking Records - Deposit And Withdrawal Records, Voided And Canceled Checks, And Other Bank-Related Documents	*Appropriate department*	**7 years**
Correspondence With Governmental And Other External Regulatory Parties	*Appropriate department*	**Permanent**
Departmental Policies, Procedures, And Other Related Documentation	*Appropriate department*	**3 years**
General Ledger Master Data	*AcctgSysAdmin*	**1 year + CFY/Permanent**
Information / Income / Corporate Tax Returns	*Corporate Tax*	**Permanent**
Payroll - Time Cards	*Payroll*	**7 years**

Payroll - Personnel-Related Documents	*Appropriate department*	**7 years**
Payroll - Record Of Payment And Deductions	*Appropriate department*	**7 years**
Payroll And Other Tax-Related Documents Filed With Federal And State Authorities (W2, 941,1042s, Etc.)	*Appropriate department*	**7 years**
Personnel Files – Departmental Copies Including Performance Measurement Documentation	*Appropriate department*	**3 years after separation**
Sap Journal Entries And Related Back-Up Documentation	*Appropriate department*	**7 years**
Sales / Excise / Miscellaneous Tax Returns And Support	*Corporate Tax*	**7 years**
Supporting Documentation For Annual Gaap Financial Reports & Interim Reporting	*Financial Reporting*	**7 years**
Supporting Documentation For Information / Income / Corporate Tax Returns	*Corporate Tax & Financial Reporting*	**7 years**
Unclaimed Property Filings And Supporting Documentation	*Corporate Tax*	**Permanent**

- Periodic Review of GAAP & Data Retention Policy (Frequency)

  _____

- Encryption Method
  - AT REST ENCRYPTION _____
  - IN TRANSIT ENCRYPTION _____
- Multi-Factor Authentication Methods

_____

➢ Network Audit Software

_____

➢ Technology To Perform Access Control

_____

_____

REQUIREMENT 4

Testing & Monitoring Effectiveness

Requirement Outcome

Firm will have a clear method viewing the ISP and testing its effectiveness vs the ever-changing landscape of cyber threats.

Date to Review Information Security Plan (ISP)

Date: _____

Who is the Qualified Person / Vendor to Make Changes & Review?

Name:
_____

Monitoring Method & Frequency (Select One)

☐ IDS / RMM (Continuous)
Vendor(s): _____

☐ Semi-Annual Network Scan & Annual Penetration Test
Vendor(s): _____

REQUIREMENT 5

Personnel Enacting Your Security Program

Requirement Outcome

Organization will have a thorough plan and strategy to conduct security awareness training and to have personnel familiar with threats that could compromise the organization.

- Security Awareness Training (SAT) Method(s)
  - 1._____
  - 2._____
  - 3._____
- Who is the qualified personnel to oversee SAT?

  _____

- Ensure SAT
  - Is relevant with recent news / threats
  - Verify that employees are taking key security measures

➢ Introduction

Our accounting firm recognizes the importance of information security and the role that our employees play in maintaining the confidentiality, integrity, and availability of our clients' data. This security awareness training policy is designed to help our employees understand the risks and threats associated with information security, and to provide them with the knowledge and skills they need to protect our clients' data.

➢ Scope

This security awareness training policy applies to all employees of our accounting firm. It also applies to any third-party contractors, vendors, or other individuals who have access to our clients' data.

➢ Objectives

The objectives of this security awareness training policy are as follows:

a. To raise awareness of the importance of information security and the risks and threats.
b. To educate employees on the best practices for safeguarding our clients' data, including but not limited to: password management, data encryption, phishing awareness, and physical security.
c. To ensure that all employees understand their roles and responsibilities in maintaining the confidentiality, integrity, and availability of our clients' data.
d. To establish a culture of security awareness throughout our accounting firm.

➢ Training Requirements

a. **Introduction to Information Security:** This module provides an overview of the importance of information security and the risks and threats associated with it.
b. **Password Management:** This module covers best practices for creating and managing strong passwords.
c. **Data Encryption:** This module explains the importance of data encryption and how to properly encrypt data.

d. **Phishing Awareness:** This module covers the basics of phishing and how to recognize and avoid phishing attacks.
e. **Physical Security:** This module explains the importance of physical security and how to properly secure physical assets.
f. In addition, all employees must complete an annual security awareness training refresher course.

➢ Reporting Incidents

All employees are required to report any suspected or actual security incidents to their immediate supervisor and the IT department as soon as possible. Examples of security incidents include but are not limited to: lost or stolen devices, unauthorized access to data, and phishing attempts.

➢ Compliance

Failure to comply with this security awareness training policy may result in disciplinary action, up to and including termination of employment.

➢ Conclusion

Our accounting firm takes information security seriously, and we are committed to providing our employees with the training and resources they need to protect our clients' data. By working together, we can create a culture of security awareness that will help us to safeguard our clients' data and maintain their trust.

REQUIREMENT 6

Oversee Providers

Requirement Outcome

Have a plan on how to oversee & audit providers and their ability to protect your own data.

- Proof your provider is capable of maintaining appropriate safeguards
  - 1. _____
  - 2. _____
  - 3. _____

- Require them by contract to maintain safeguards

- Periodically Assess Providers (Frequency)

  _____

  - Are they able to showcase adequacy of safeguards?

    _____

  - What potential risk exists with them?

    _____

Policies for Choosing Vendors

- Identify The Need

  The accounting firm should identify the need for third-party software and vendors. This may include areas such as bookkeeping, payroll, tax preparation, and audit support.

- Define Evaluation Criteria

  The accounting firm should define evaluation criteria that are relevant to their needs. These criteria may include functionality, security, support, scalability, and cost.

- Research Potential Vendors

  The accounting firm should conduct research to identify potential vendors that meet the defined evaluation criteria. This research may include online searches, reviews, and recommendations from other firms in the industry.

- Request Information

  The accounting firm should request information from potential vendors that will help evaluate their software and services. This information may include product demos, feature lists, pricing, and service level agreements.

- Evaluate Vendor Responses

  The accounting firm should evaluate the responses from potential vendors against the defined evaluation criteria. This may involve scoring vendors on each criterion to determine which ones meet the firm's needs.

- Perform Due Diligence

  The accounting firm should perform due diligence on potential vendors to ensure they are reputable and reliable. This may include checking references, reviewing financial statements, and conducting background checks.

- Negotiate Contracts

  The accounting firm should negotiate contracts with selected vendors that specify the terms and conditions of the relationship. This may include service level agreements, pricing, and security requirements.

- Implement Software & Services

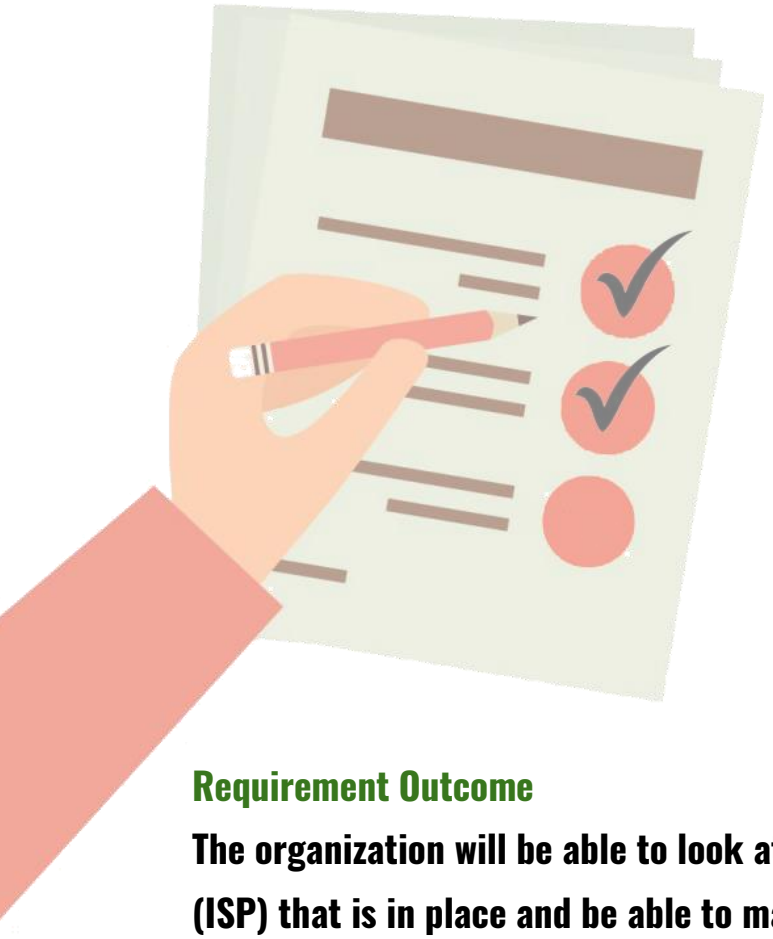
  Once contracts have been finalized, the accounting firm should implement the selected software and services. This may involve training employees, setting up access controls, and configuring software settings.

- Monitor Performance

  The accounting firm should monitor the performance of the software and services to ensure they meet the defined criteria. This may involve conducting regular audits, reviewing user feedback, and tracking system uptime.

- Conduct Regular Reviews

  The accounting firm should conduct regular reviews of the software and services to ensure they continue to meet their needs. This may involve revisiting the defined evaluation criteria and conducting a new evaluation of potential vendors.



REQUIREMENT 7

Evaluate and Adjust Security Program

Requirement Outcome

The organization will be able to look at the current Information Security Program (ISP) that is in place and be able to make corrections based on new findings and audits.

→ FTC References Requirement 4: Testing & Monitoring Effectiveness
→ Take the assessment and modify
→ FTC References Requirement 2 for addressing risk assessment
Last Assessment Performed (Date): _____
Assessment Evaluation (Frequency): _____
Modification Execution (Frequency): _____
Identify Material Changes to Company Since Last Assessment:

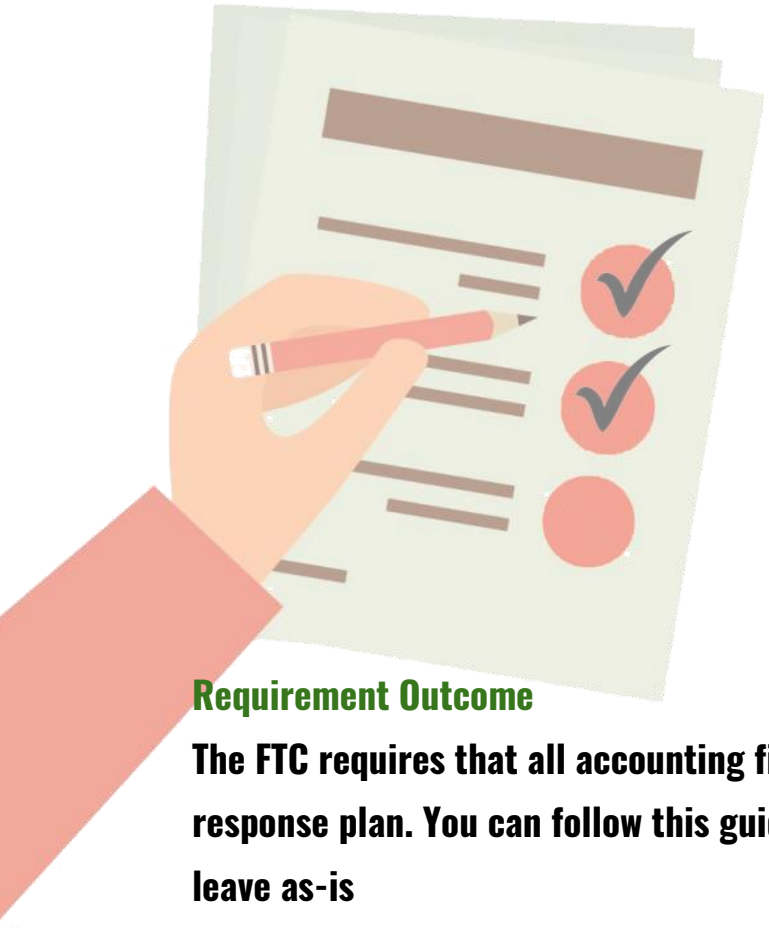
- _____
- _____

What material impact does the risk assessment list?

- _____
- _____

What needs to change as a result of the findings?

- _____
- _____



REQUIREMENT 8

Written Incident Response Plan

Requirement Outcome

The FTC requires that all accounting firms have and maintain a written incident response plan. You can follow this guideline to construct one for your company or leave as-is

01

The plan also aims to minimize the impact of security incidents or data breaches, including reducing the risk of harm to affected individuals and preventing further unauthorized access or disclosure of sensitive information.

02

The goal of this FTC written incident response plan is to provide a clear, efficient, and effective response to security incidents or data breaches that may affect the organization or its customers. The plan should include procedures for identifying, containing, investigating, and resolving security incidents, as well as communicating with customers, regulatory authorities, and other stakeholders.

03

Additionally, the plan should aim to improve the organization's security posture by identifying vulnerabilities and implementing measures to prevent similar incidents from occurring in the future.

04

Finally, the plan should ensure compliance with applicable laws, regulations, and industry standards governing incident response and data protection.

- ➢ The internal processes your company will activate in response to a security event
    a. Establish an incident response team with clearly defined roles and responsibilities
    b. Identify the nature and scope of the security incident
    c. Contain the incident by disconnecting affected systems from the network, isolating compromised devices, or other appropriate measures
    d. Gather and preserve evidence to assist in investigating the incident
    e. Notify and coordinate with law enforcement, regulatory agencies, and other relevant stakeholders as required by law or company policy
    f. Assess the potential impact of the incident, including the risk of harm to affected individuals and the organization's business operations
    g. Develop and implement a remediation plan, including steps to restore affected systems, mitigate harm to affected individuals, and prevent similar incidents from occurring in the future
    h. Communicate with customers, employees, and other stakeholders as appropriate, providing accurate and timely information about the incident and steps taken to address it
    i. Review and evaluate the incident response process and update policies and procedures as necessary to improve future incident response efforts.
- ➢ Clear roles, responsibilities, and levels of decision-making authority
    - ➢ Incident Response Team (IRT):
        - The IRT should be established with clearly defined roles and responsibilities.
        - The team should consist of individuals with the necessary skills and expertise to handle the incident.
        - The IRT should be responsible for coordinating the response to the data breach.
        - Incident Response Coordinator: _____
    - ➢ The Incident Response Coordinator should be identified and have the ultimate responsibility for managing the incident response.

        - The Incident Response Coordinator should have decision-making authority to determine the scope of the incident and the necessary steps to contain, investigate, and remediate the incident.

    - IT and Technical Staff:
        - IT and Technical staff should be responsible for containing the incident, identifying the root cause, and remediating the incident.
        - IT and Technical staff should work closely with the IRT to ensure effective coordination and communication.
    - Legal and Compliance:
        - Legal and compliance staff should be responsible for ensuring compliance with legal and regulatory requirements related to the data breach.
        - Legal and compliance staff should work closely with the IRT to provide guidance on legal and regulatory requirements related to the breach.
    - Public Relations:
        - Public Relations staff should be responsible for managing communication with stakeholders, including customers, partners, and the media.
        - Public Relations staff should work closely with the IRT to ensure effective communication and messaging during and after the breach.
    - Communications and information sharing inside/outside your company:
        - _____
    - A process to fix any identified weakness in your systems and controls:
        - _____
    - Procedure for documenting security events and your company's response:
        - _____
    - A post mortem of what happened and a revision of your incident response & ISP.
        - _____

REQUIREMENT 9

Require Your Qualified Vendor / Individual to Report to Your Board of Directors

Requirement Outcome

Have a set plan for when the vendor or qualified individual reports to your board of directors.

The report shall include the following information:

1. The overall status of the information security program (ISP) and your compliance
    a. List out all requirements and their adherence
    b. Showcase the number of attacks blocked
    c. Demonstrate the protocols that are in place
    d. Make recommendations based on the current status
2. Material matters related to the information security program,
    a. Risk assessment
    b. Risk Management
    c. Control Decisions
    d. Service Provider Arrangements
    e. Results of Testing
    f. Security Events or Violations and Management's Response
    g. Recommendations for Change

IRS Publications on Data Security

- **Publication 5293:** Data Security Resource Guide for Tax Professionals
- **Publication 1345:** Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns
- **Publication 4557:** Safeguarding Taxpayer Data Quick Reference Guide for Business

IRS Publication 5293

Data Security Resource Guide for Tax Professionals

1. Learn to recognize phishing emails, particularly those pretending to be from the IRS, tax software providers, or cloud storage providers. Never open suspicious links or attachments.
2. Create a data security plan using IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security – The Fundamentals, by the National Institute of Standards and Technology.
3. Install anti-malware/anti-virus security software on all devices and keep it updated.
4. Use strong and unique passwords of 8 or more mixed characters and password-protect all wireless devices. Change passwords periodically.
5. Encrypt all sensitive files/emails and use strong password protections.
6. Back up sensitive data to a safe and secure external source that is not connected full-time to a network.
7. Make a final review of return information, especially direct deposit information, before e-filing.
8. Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
9. Limit access to taxpayer data to individuals who need to know.

10. Check IRS e-Services account weekly for the number of returns filed with EFIN.
11. Report any data thefts or losses to the appropriate IRS Stakeholder Liaison.
12. Stay connected to the IRS through subscriptions to e-News for Tax Professionals, QuickAlerts, and Social Media.
13. Learn the signs of data theft, including rejected e-filed returns, unexpected authentication letters, unrequested refunds or tax transcripts, and notices of unauthorized account access.
14. Track daily e-file acknowledgments and weekly EFIN usage. Contact the e-Help desk if the numbers are off.
15. Check PTIN account(s) for a weekly report of returns filed if you are a Circular 230 practitioner or annual filing season program participant filing 50 or more returns per year.
16. Keep your Centralized Authorization File (CAF) Number up-to-date and remove authorizations for taxpayers who are no longer your clients.
17. Create IRS online accounts using the two-factor Secure Access authentication to prevent account takeovers.

IRS Publication 1345

Authorized IRS E-File Providers of Individual Income Tax Returns

1. Use strong passwords and change them regularly
2. Keep all software and hardware up-to-date with security patches and updates
3. Use antivirus and anti-malware software on all company systems
4. Use firewalls and encryption to protect personal information stored on company systems
5. Back up important data regularly and store backups in a secure location
6. Limit access to personal and financial information on a need-to-know basis
7. Train employees on security awareness and best practices
8. Use secure methods for transmitting personal and financial information
9. Develop and implement a disaster recovery plan
10. Develop and implement policies and procedures for securely disposing of information
11. Use multi-factor authentication for accessing personal and financial information
12. Implement physical security measures to protect information stored on company premises
13. Regularly review and update security policies and procedures
14. Develop and implement procedures for responding to security incidents
15. Limit the collection, use, and retention of personal and financial information to what is necessary for business purposes
16. Conduct background checks on employees with access to personal and financial information
17. Monitor networks and systems for suspicious activity
18. Use secure methods for disposing of personal and financial information
19. Develop and implement procedures for securely transferring personal and financial information to third-party service providers
20. Develop and implement a data breach response plan

21. Implement controls to detect, prevent, and respond to attacks, intrusions, or other unauthorized access to personal and financial information
22. Develop and implement procedures for securely storing and destroying paper documents
23. Use secure methods for accessing company systems and data remotely
24. Implement controls to prevent unauthorized access to company systems and data
25. Develop and implement a mobile device policy for employees
26. Train employees on how to recognize and avoid phishing scams and other attacks
27. Use strong authentication mechanisms for all company accounts
28. Use digital signatures for sensitive documents and transactions
29. Develop and implement procedures for securely storing and transferring encryption keys
30. Implement network segmentation to limit access to sensitive information
31. Use secure email services to send and receive sensitive information
32. Implement web filtering to block malicious websites and content
33. Regularly review and update network and system logs
34. Develop and implement procedures for securely disposing of hardware and storage media that contain personal and financial information
35. Use secure file transfer protocols for data transfer

IRS PUBLICATION 4557

Safeguarding Taxpayer Data

1. Keep all software and hardware up-to-date with security patches and updates
2. Use strong passwords and change them regularly
3. Install and use antivirus and anti-malware software on all company systems
4. Use firewalls and encryption to protect personal information stored on company systems
5. Back up important data regularly and store backups in a secure location
6. Limit access to personal and financial information on a need-to-know basis
7. Train employees on security awareness and best practices
8. Use secure methods for transmitting personal and financial information
9. Develop and implement a disaster recovery plan
10. Develop and implement policies and procedures for securely disposing of personal and financial information
11. Use multi-factor authentication for accessing personal and financial information
12. Implement physical security measures to protect personal and financial information stored on company premises
13. Regularly review and update security policies and procedures
14. Develop and implement procedures for responding to security incidents
15. Limit the collection, use, and retention of personal and financial information to what is necessary for business purposes
16. Conduct background checks on employees with access to personal and financial information
17. Monitor networks and systems for suspicious activity
18. Use secure methods for disposing of personal and financial information
19. Develop and implement procedures for securely transferring personal and financial information to third-party service providers

20. Develop and implement a data breach response plan
21. Implement controls to detect, prevent, and respond to attacks, intrusions, or other unauthorized access to personal and financial information
22. Develop and implement procedures for securely storing and destroying paper documents that contain personal and financial information
23. Use secure methods for accessing company systems and data remotely
24. Implement controls to prevent unauthorized access to company systems and data
25. Develop and implement a mobile device policy for employees
26. Train employees on how to recognize and avoid phishing scams and other social engineering attacks
27. Use strong authentication mechanisms for all company accounts
28. Use digital signatures for sensitive documents and transactions
29. Develop and implement procedures for securely storing and transferring encryption keys
30. Implement network segmentation to limit access to sensitive information
31. Use secure email services to send and receive sensitive information
32. Implement web filtering to block malicious websites and content
33. Regularly review and update network and system logs

GLOSSARY

Here are some definitions from the Safeguards Rule. Consult 16 C.F.R. § 314.2 for more definitions.

Authorized user means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.

Customer information means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Encryption means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material. Data at rest similar to on a hard drive or storage device. In transit would be sending information across the network to other employees or clients. Includes emails.

Incident Detection System means a system / software that uses various sensors and algorithms to automatically identify and alert operators to unusual events or situations in real-time. It is commonly used to detect and respond to incidents quickly and effectively. The system can identify incidents such as unauthorized access, policy changes, security breaches, among others. This helps to reduce response time and improve safety and security in the firm.

Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Information system means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

Multi-factor authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics.

Nonpublic personal information (NPI) means: (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

Security event means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such an information system, or customer information held in physical form.

Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to an accounting firm.