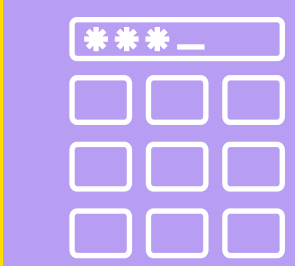
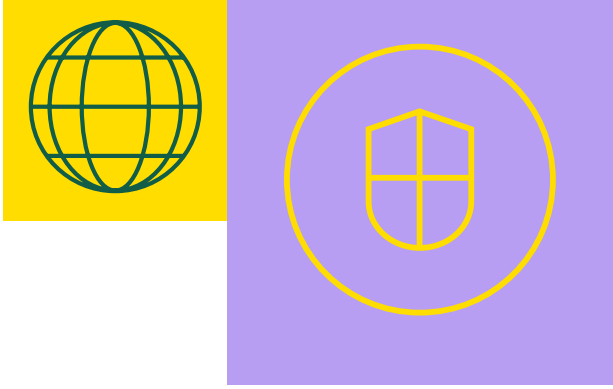
Practice Protect University

Accounting Data Security Standard
CERTIFIED

IRS 4557 Data Security Plan Guidelines

BY Practice Protect
MORE TRUST. LESS RISK.



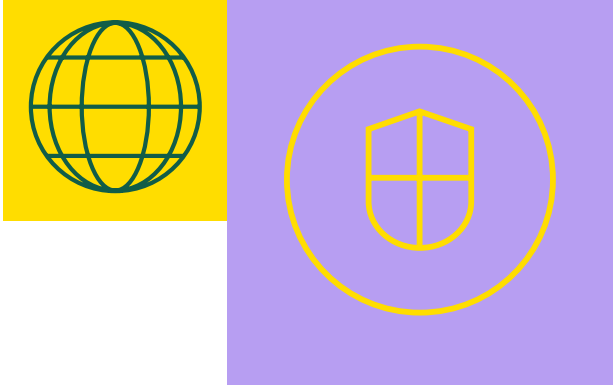


What should a compliant data security plan include?

At Practice Protect, we offer a data security plan template for all clients, as a part of our Practice Protect University(PPU). The PPU is free for all customers and contains a wealth of resources and templates that assist accounting firms in compliance, training, digital security and up-skilling. We consulted with top-tier attorneys to create an industry-standard data security plan so that you wouldn't have to.

For those readers who are not Practice Protect customers, we still want to help. This document outlines a list of what should go into your data security plan.

Data security plan sections



PART I - RISK & REMEDIATION

1. A risk assessment must be completed
2. Identify the risks and impacts of unauthorized data use and access
3. Determine systems vulnerability of your firm
4. Highlight a list of actions to reduce vulnerability

PART II - SYSTEMS, SOFTWARE & POLICIES

5. Software and hardware safeguards in place
6. Password management procedures
7. Email security and email security training
8. Privacy notices and practice policy disclosures for clients
9. The use of encryption in sharing of sensitive data
10. The use of non disclosure agreement
11. Wireless networks and internet usage monitoring
12. Use and storage of backups

PART III - FACILITIES & CONTRACTORS

13. Facilities security protection and procedures in event of disaster
14. Written security policies of all service providers
15. Third party contractors security processes and rules of behavior
16. The use of personal and company machines

PART IV - PEOPLE & TRAINING

17. Personnel security including rules of behavior
18. Responsible data security personnel
19. Self-assessment protocols and cadence for employees
20. Ongoing security training for personnel
21. Employee termination protocol
22. Exit interview templates for terminated employees
23. Enforcement of need-to-know access of sensitive data internally
24. Training your clients

PART V - PROTOCOL & MONITORING

25. Annual review protocol
26. Automated and manual systems security
27. Written contingency plan in event of disruption
28. Management of active and inactive digital accounts
29. Disposal of sensitive data on contract termination with client
30. Monitor EFIN/PTINs

Part I - Risk & remediation

1. A risk assessment must be completed

A risk assessment can be conducted internally or externally and takes stock of every device, person, software piece, external stakeholder, documented process, and compliance system. This will include everything from IT servers to cloud infrastructure providers. The purpose of a risk assessment is to identify every potential risk vector in the business and to take stock of every angle that requires data security process embedded. Use a scoring methodology to determine the level of risk associated with each risk audit item, and how you rate in data security effectiveness. The results and data of your last risk assessment should be present within your data security plan.

2. Identify the risks and impacts of unauthorized data use and access

From the assessment, grade each vulnerability identified from high-impact to low-impact and high-urgency to low-urgency so that you can prioritize remediation tasks. Uncovering the risks and potential impact will help generate a clear business case for each remediation effort, and importantly, allow you to understand the risk appetite alignment in your business.

3. Determine systems vulnerability of your firm & 4. Highlight a list of actions to reduce vulnerability

An audit of all systems by a qualified professional will expose any vulnerability in your systems. The data security plan must address each of these as well as plans to fix and re-mediate. The IRS 4557 guidelines sets the bar high - particularly with systems that house and/or transfer sensitive client data within and outside of your business.

Part 2 - Systems, software & policies

5. Software and hardware safeguards in place

Define the software and hardware security measures that been put in place to monitor, respond and optimize data security in your firm. From anti-malware/anti-virus to anti-spyware, firewalls, drive encryption software, and advanced monitoring tools.

6. Password management procedures

Outline what password management software and protocols are in place to govern the use of sensitive login data within your business. This is particularly important to the 4557 guidelines. Strong passwords should be mandated with character minimums and use of special / alphanumeric characters (at least NIST standard). However, password creation is only part of the strategy. Password rotation and sharing should be governed internally.

7. Email security and email security training

Outline what email platforms are used and what security plugins / monitoring software is in place. Discuss any email-layer encryption and staff training on how to avoid phishing scams and the like.

8. Privacy notices and practice policy disclosures for clients

Include your privacy policy and data security policies (disclosures) that you publish on your website, in your client agreements and within new client on-boarding.

9. The use of encryption in sharing of sensitive data

Outline what encryption is used throughout the business when sharing sensitive information. The 4557 guidelines mandate the encryption of sensitive files/emails, especially those relating to identity.

10. The use of non disclosure agreements

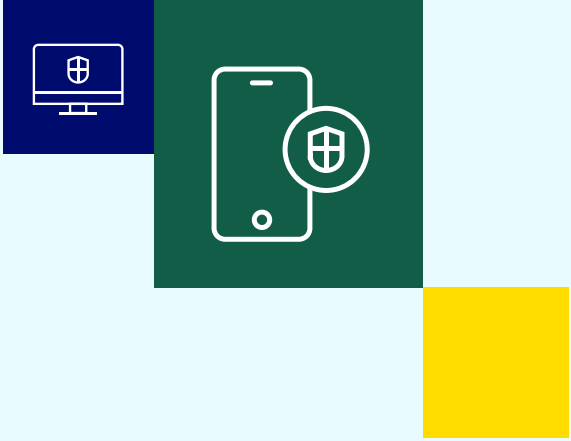
Include internal and external non-disclosure agreements along with your protocol for how they are used throughout your firm. New employees should agree to these standards, particularly considering the sensitivity of client information.

11. Wireless networks and internet usage monitoring

Thieves can steal your data without your knowledge which is why network security is an essential part of any data security plan. From router naming to wireless access protocols, WEP (private connections), it's important to define how you as a company safely operate. Define how wireless networks are accessed and what processes / approvals are in place for public WiFi or at-home.

12. Use and storage of backups

Storage and backups will be documented within your data security plan - as well as redundancy, off site storage and appropriate security protocols in place for the storage and backup of your data. Firms are encouraged to considered external backups not connected to the primary network.



Part 3 - Facilities & contractors

13. Facilities security protection and procedures in event of disaster

Take inventory of hardware and facility assets - as well as appropriate physical and digital security processes. Outline response in event of common disasters, which are relevant to your geography.

14. Written security policies of all service providers

The 4557 guidelines stipulates that you must also ensure contractors and service providers have adequate data security systems and policies in place, particularly if your data runs through their systems in any way.

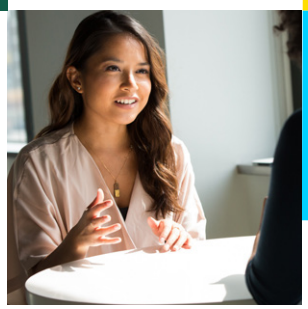
15. Third party contractors security processes and rules of behavior

A data security checklist and contractor behavior policy will be included in your data security plan and distributed to all contractors. This will govern sharing of data and access to sensitive information, as well as access to systems and servers.

16. The use of personal and company machines

Outline what policies are in place for the user of company and personal machines.

Part 4 - People & training



17. Personnel security including rules of behavior

A data security checklist and personnel behavior policy will be included in your data security plan and distributed to all employees. This will govern sharing of data and access to sensitive login information for clients, as well as machine access etc.

18. Responsible data security personnel

A data security officer will be appointed and identified in your data security plan. It is recommended that this person is responsibly trained in cybersecurity and data security protocol as well as the relevant compliance benchmarks for the accounting industry. They will arrange and execute internal training programs for staff and be responsible for systems security reporting.

19. Self-assessment protocols and cadence for employees

Include the self assessment checklists and surveys which are routinely distributed and measured to ensure your employees follow security processes.

20. Ongoing security training for personnel

Include a security training schedule for personnel and where appropriate, the training material / training provider that you use.

21. Employee termination protocol

Outline an employee off-boarding checklist including how quickly employees are removed from systems and fail-safe measures in place to mitigate ongoing security risks.

22 Exit interview templates for terminated employees

Include exit interview template which includes a completion of data-security off-boarding. The IRS encourages all tax preparers to have a protocol for data wiping machines and devices of sensitive information at the completion of employment

23. Enforcement of need-to-know access of sensitive data internally

Define how sensitive data is partitioned, quarantined and accessed on a need-to-know basis. From file structures to sharing access. The expectation is that sensitive information is only available to those that require access and not to the firm as a whole.

24. Training your clients

Clients also present a risk vector for accounting firms. Communicating the importance of data security regularly to customers helps reinforce how important it is to you (for their peace of mind) and reminds them to think twice before transmitting information that is sensitive to you through less secure pathways.

Part 5 - Protocol & monitoring

25. Annual review protocol

The data security plan is not intended to be set-and-forget but instead, a live and active document. To achieve this, regular reviews should be coordinated and pre-planned (outlined in your plan). We recommend either 6-monthly or annually.

26. Automated and manual systems security

Outline automate systems monitoring and security which is in place, as well as any manual processes that you perform regularly.

27. Written contingency plan in event of disruption

In the event of a cyber-breach, what contingencies are set up to protect further damage and retain operational continuity? Firms are required to report any suspected data theft or data loss immediately to the appropriate IRS Stakeholder Liason and also to StateAlert@taxadmin.org.

28. Management of active and inactive digital accounts

Inventory of all digital accounts owned, both active and inactive. Outline the process of how these are managed and what risk mitigation is in place for cyber breaches and unauthorized access.

29. Disposal of sensitive data on contract termination with client

Outline how sensitive data is disposed of or retained on termination with client. What communication protocols are in place to notify the client of data disposal?

30. Monitor EFIN/PTINs

The IRS encourages all tax preparers to run weekly reports on tax returns filed with your electronic filing identification number (EFIN) or preparer tax identification numbers (PTIN). Authorizations for taxpayers who are no longer clients should be removed regularly.

“Preserving confidentiality is a core professional duty.”

— **Journal of Accountancy**

Practice Protect University

Accounting Data Security Standard
CERTIFIED

Practice Protect
MORE TRUST. LESS RISK.

Book a demo: **www.Practiceprotect.com**

www.practiceprotect.com/data-security-plan/

hello@practiceprotect.com