



IRS PUBLICATION 4557 COMPLIANCE CHECKLIST

1

COMPLETE THE COURSE

- Take the course: [Complying with IRS Publication 4557](#)

2

CONDUCT BACKGROUND CHECKS

- If your firm has not done this already, conduct Background Checks on all employees and contractors. Download [this document](#) for instructions.

3

REVIEW & MODIFY REQUIRED POLICES AND PROCEDURES

- Download the following IRS-compliant sample policies, attachments and procedures. Fill in your firm's information and edit if necessary.
 - Sample [Password Policy](#).
 - Sample [Rules of Behavior and Conduct Safeguarding Client PII and Customer Information](#)
 - Sample [Securing Customer and Firm Data Policy](#).
 - Sample [Record Retention Policy](#).
 - Sample [Security Breach Procedures and Notifications Policy](#).

4

GET YOUR STAFF ON BOARD!

- Schedule a firm-wide Kickoff Meeting for staff and contractors.
 - Download and modify [these slides](#) to explain the importance of security and to help train your staff (one of the requirements of your WISP).
- After the meeting, ensure every employee/contractor signs and returns:
 - [Employee/Contractor Acknowledgement of Understanding](#)
 - [Non-Disclosure Agreement](#)

5

TAKE INVENTORY AND EVALUATE YOUR SOLUTIONS

- Use the [Technology Resource Guide](#) - what solutions do you need to add to your firm?
- Consider whether you will handle the security software requirements yourself, or if you would like help.
 - Schedule appointments with software suppliers (if needed).
 - Alternatively, if you prefer to "vend it out" schedule time with your preferred IT Managed Service Provider.



IRS PUBLICATION 4557 COMPLIANCE CHECKLIST

6

COMPLETE YOUR WISP

- Download your preferred WISP and modify to fit your firm's needs:
 - [IRS WISP](#) - relevant for any firm size
 - [Tech 4 Accountants WISP](#) - good for any small - medium sized firm
 - [Large Firm WISP](#) - good for firms with an internal IT department
- Complete and attach all required attachments:
 - Attachment A: [Record Retention Policy](#).
 - Attachment B: [Rules of Behavior and Conduct Safeguarding Client PII & Customer Information](#)
 - Attachment C: [Security Breach Procedures and Notifications](#)
 - Attachment D: [Employee/Contractor Acknowledgement of Understanding](#).
 - COMPLETE: Attachment E: [Firm Hardware and Software Inventory containing PII Data & Customer Information](#)
 - COMPLETE: Attachment F: [Firm Employees Authorized to Access PII & Customer Information](#)

7

GET YOUR CLIENTS ON BOARD

- Share the good news with clients!
 - Roll out your preferred secure solution for clients.
 - Inform them that you are now in compliance with the IRS and FTC regulations, and ask them to do their part to ensure success.
 - Leverage [sample language here](#), and modify it to suit your firm's needs.

8

ANNUAL ACTIONS TO SCHEDULE

- Annual required Security Training for staff.
- Review and update all policies pertaining to security, including your WISP.
- Review and update hardware and software inventories containing PII and Customer Data. (Attachment E)
- Review and update the list of firm employees authorized to access PII and Customer Information. (Attachment F)
- Ensure that appropriate data is destroyed in accordance with firm policy.