Form **15272**
(September 2020)

Department of the Treasury - Internal Revenue Service

VITA/TCE Security Plan

Purpose: Enhance and maintain the security of taxpayer information utilized at a VITA/TCE location by adhering to the security requirements outlined in Publication 4299, Privacy, Confidentiality, and Civil Rights – A Public Trust. Partners and site coordinators are responsible for protecting taxpayers' private information by following IRS security requirements. Publication 4299 was updated to explain how site coordinators should validate that requirements are followed.

Directions: The security plan must be completed for all sites, then signed by the site coordinator and partner. Each plan must be approved by the SPEC territory manager or designee prior to the opening of the site. Sites can use this form or a similar document that captures the same information. A copy of the approved security plan must be maintained at the site and by the territory office.

Site name	Site address

Type of software used

☐ IRS software - TaxSlayer ☐ Online ☐ Desktop ☐ Other *(list name)* _____

Date completed	Completed by

	Name	Telephone Number	Email Address
Partner			
Site Coordinator			
Alternate Site Coordinator			

Site/Virtual location

Complete equipment inventory log

	# IRS Owned	# Partner Owned	# Volunteer Owned
Laptops			
Portable mass storage devices			
Other			

1. Are procedures being followed at the site to confirm all volunteers are aware of the security requirements in Publication 4299, *Privacy, Confidentiality, and Civil Rights (i.e., privacy during the interview, validating taxpayer identity and identification numbers)*? If no, explain ☐ Yes ☐ No

2. If using a wireless network at the site, are requirements being followed from Publication 4299 to restrict unauthorized access to the site's wireless network? If no, explain ☐ Yes ☐ No

3. Are software access privileges limited based on the volunteers assigned roles as outlined in Publication 4299 *(i.e., security templates for preparers, quality reviewers, super users, etc.)*? If no, explain ☐ Yes ☐ No

4. Are security requirements followed for protecting all equipment *(computers, printers, flash drives, thumb drives, external hard drives, etc.)* to ensure proper use, storage and disposal at the site during and after site operating hours? If no, explain ☐ Yes ☐ No

5. Are there site procedures to limit unauthorized access to taxpayer information *(i.e., positioning computer screens, protecting taxpayer documents and preventing others from hearing sensitive information)* and to ensure privacy? If no, explain ☐ Yes ☐ No

6. Does the site coordinator generally restrict volunteer access to the tax preparation software *(changing active to inactive)* after site operating hours as described in Publication 4299? If no, explain ☐ Yes ☐ No

7. Is the site coordinator aware of the process for reporting lost and/or stolen computer *(both IRS loaned and partner owned)* immediately but no later than the next business day after confirmation of the incident? If no, explain ☐ Yes ☐ No

8. Are you aware of the procedures for reporting a data breach to your SPEC Territory Office as described in Publication 4299? If no, explain ☐ Yes ☐ No

9. Is physical and/or electronic taxpayer Personally Identifiable Information (PII) in your possession properly secured and/or disposed of when no longer needed? If no, explain ☐ Yes ☐ No

10. Are you aware of how to report unethical violations as outlined in the Publication 4961, *Volunteer Standards of Conduct-Ethics Training*? If no, explain ☐ Yes ☐ No

11. At the end of the filing season, are the guidelines in Publication 1084, *VITA/TCE Site Coordinator Handbook*, followed for closing the site? If no, explain ☐ Yes ☐ No

12. If you operate a Virtual VITA/TCE site, was a written Virtual VITA/TCE plan created and submitted for approval to your SPEC Territory Office? If no, explain ☐ Yes ☐ No ☐ N/A

Coordinator name	Signature	Date
Partner name	Signature	Date
Relationship Manager's name	Signature	Date
Territory Manager's name	Signature	Date