Privacy, Confidentiality, and Civil Rights

- A Public Trust

*"...ensuring IRS volunteers and their partnering organizations **safeguard taxpayer information** and understand their responsibilities ..."*

Publication 4299 (Rev. 10-2021) Catalog Number 38128T Department of the Treasury **Internal Revenue Service** www.irs.gov

TABLE OF CONTENTS

TABLE OF CONTENTS

Privacy, Confidentiality, and Civil Rights – A Public Trust

Introduction

The Internal Revenue Service (IRS) sponsors the Volunteer Income Tax Assistance (VITA) and the Tax Counseling for the Elderly (TCE) Programs that provides free tax return preparation for low to moderate income and elderly taxpayers. Details governing the operation of these two programs exist in various resource materials; however, both programs must guarantee confidentiality of taxpayer information to protect public trust. This document addresses areas where partners and volunteers need to exhibit diligence to details when administering the requirements of these programs.

Section 7216 of the Internal Revenue Code (IRC) and a related provision, IRC 6713, provide penalties against tax return preparer who make unauthorized use or disclosure of tax return information. A tax return preparer covered by IRC 7216 and 6713 can include a person who prepares tax returns or assists in preparing tax returns, whether or not a fee is charged for preparing a tax return.

Background

Information provided by individual taxpayers to a VITA/TCE volunteer is not considered “return information” protected by IRC 6103 until the IRS receives, records or collects it. However, VITA/TCE volunteers are subject to the criminal penalty provisions of 18 USC 1905 for any improper disclosures of this information. It is critical to the programs’ success to ensure volunteers and their partnering organizations safeguard taxpayer information and understand their responsibilities.

Taxpayers using volunteer program services provide Personally Identifiable Information (PII) to the volunteers, such as names, addresses, Social Security Numbers (SSN), birth dates, and bank account information. This type of information is a prime target for identity theft. Therefore, partners and volunteers must keep the information confidential and protect it from unauthorized individuals and misuse. Partners and volunteers must minimize the retention of any taxpayer PII records unless the taxpayer provides written consent to disclose and use as explained under Taxpayer Consents.

Protection Against Legal Action

Public Law 105-19, Volunteer Protection Act of 1997 (VPA) generally protects volunteers from liability for negligent acts they perform within the scope of their responsibilities in the organization for whom they volunteer. The VPA is not owned or written exclusively for Internal Revenue Service. This is a Public Law and relates to organizations that use volunteers to provide services.

Under the VPA, a “volunteer” is an individual performing services for a nonprofit organization or a governmental entity (including as a director, officer, trustee, or direct service volunteer) who does not receive for these services more than $500 total in a year from the organization or entity as:

a. Compensation (other than reasonable reimbursement or allowance for expenses actually incurred), or
b. Any other thing of value in lieu of compensation.

Although an individual may not fall under the VPA definition of a “volunteer,” which means they may not be protected under the VPA, the VITA/TCE Programs still considers them volunteers. To ensure protection, those who do not fit this VPA volunteer definition must seek advice from their sponsoring organization’s attorneys to determine liability protection rights.

Penalty for Unauthorized Disclosures or Uses

IRC 7216(a) imposes criminal penalties on tax return preparers who knowingly or recklessly make unauthorized disclosures or uses of information furnished in connection with the preparation of an income tax return. A violation of IRC 7216 is a misdemeanor, with a maximum penalty of up to one year imprisonment or a fine of not more than $1,000, or both, together with the cost of prosecution.

Privacy and Confidentiality – Key Principles

To maintain program integrity and provide for reasonable protection of information provided by the taxpayers serviced through the VITA/TCE Programs, it is essential that partners and volunteers adhere to the strictest standards of ethical conduct and the following key principles.

- Partners must ensure site coordinators are aware of security requirements covered in Publication 4299 and hold discussions with volunteers at the sites to review the requirements.
- Partners and volunteers must keep confidential the information provided for tax return preparation.
- Partners and volunteers must protect physical and electronic data gathered for tax return preparation both during and after the filing season.
- Partners using or disclosing taxpayer data for purposes other than current, prior, or subsequent year tax return preparation must secure the taxpayer's consent to use or disclose their data. Refer to the section on Taxypayer Consents later in this publication for exceptions to securing the taxpayer's consent.
- Partners and volunteers must delete taxpayer information on all computers (Bring Your Own Device (BYOD), partner owned and IRS loaned) after filing season tax return preparation activities end.
- Partners and site coordinators must keep confidential all personal information the taxpayer provides.

Taxpayer Information

Partners and volunteers must keep confidential the information taxpayers provide for tax return preparation.

Taxpayers Must Participate in Return Preparation

Volunteers must prepare all tax returns at the site with the taxpayer present unless (1) preparing a joint return for a married couple with one taxpayer present at the site or (2) preparing a return for a minor child in the presence of the child's parent or guardian or (3) when using an approved Virtual VITA/TCE service model (please note the exceptions for Virtual VITA/TCE service model options in the paragraph below). Otherwise, VITA/TCE sites must not prepare a tax return without the taxpayer's participation even if the taxpayer authorized another person to represent them for the preparation of a tax return.

Exception: Having the taxpayer present in the preparer's site when the tax return is being prepared is not always possible. In these cases, Virtual VITA/TCE processes offer alternative options to prepare returns without face to face contact with the taxpayer. Certified volunteers may interview taxpayers over the phone while preparing their returns. The alternative process partners choose to prepare returns must be approved by the responsible IRS Territory Manager to ensure all procedures are in place as described in the Quality Site Requirements (QSR). Most importantly, the taxpayer's and government's interests must be properly protected. In some cases, the taxpayer information must be left at the site while the return is prepared and then returned to the taxpayer. Adequate security and privacy is expected to ensure taxpayer records are properly safeguarded. Refer to Publication 5450, VITA/TCE Site Operations, for more information on Virtual VITA/TCE processes.

In situations where a taxpayer presents information not sufficient to complete the return, the volunteer must return all documents to the taxpayer with instructions to return to the site with all required documents for completion of the tax return.

Privacy During the Interview

To the extent possible, arrange tax preparation assistance areas to prevent others from easily overhearing or viewing the information under discussion. Partners must ensure that taxpayer privacy is protected when sharing personally identifiable information (PII) such as SSNs, address, bank account numbers, etc. During conversations with taxpayers, volunteers must not discuss PII information out loud. For example, volunteers can point to the computer screen or supporting document containing the PII information and the taxpayer could verify if the information is correct. While arranging the layout of the VITA/TCE site, plan how you will accommodate taxpayers who may need more space or privacy. (Examples: a deaf or hard of hearing taxpayer with one or more sign language interpreters, a limited English proficient taxpayer that requires a language interpreter, a blind/visually impaired taxpayer with a service dog, or a taxpayer in a wheelchair). Refer to the **Site Coordinator's Corner** on **www.irs.gov** for additional information on how to accommodate taxpayers with disabilities and limited English proficiency. Volunteers requesting assistance to complete a tax return must maintain privacy during discussions.

Requesting the Information

When preparing tax returns, only request necessary and relevant information. The taxpayer provides their information trusting the volunteer will not share or use the information in an unauthorized manner.

Tax return preparation requires taxpayer's to provide information such as name, address, Social Security Numbers (SSN), birth dates, marital status, bank account information for direct deposit, and other basic information. Volunteers must use documents such as government issued photo ID, employer ID, school ID, social security cards, and ITIN letters to ensure identity and accuracy.

Validating Taxpayer(s) Identity and Identification Number(s)

All volunteers must follow validation procedures prior to tax return preparation and before a taxpayer may sign or receive a copy of a VITA/TCE prepared tax return.

IRS-tax law certified volunteers preparing tax returns must confirm the identity of each taxpayer signing the tax return to prevent identity theft and tax fraud. The volunteer must review an original photo identification (ID) such as valid driver's license (U.S.), employer ID, school ID, state ID (U.S.), Military ID, national ID, visa, or passport. Volunteers must use judgment when accepting any other valid form of identification. If a taxpayer cannot substantiate his/her identity, or if the volunteer is uncomfortable accepting the items presented as proof of identity, the taxpayer must be advised to return with an acceptable form of identification. Exceptions to requiring an original photo ID must only be made under extreme circumstances and require site coordinator approval. For example, the site coordinator can confirm the identity of an elderly person with a disability who has an expired driver's license or passport but provides a valid birth certificate.

IRS-tax law certified volunteers preparing tax returns must also verify the taxpayer identification numbers (TIN) and the correct spelling of names of all individuals listed on the tax return. Taxpayers must provide original or copies (paper or electronic) of social security cards or an acceptable substitute such as a letter from the Social Security Administration (SSA), Form SSA-1099, and/or any other verification issued from the SSA. SSA verification documents with a truncated SSN (such as ***-**-1234) can be used as acceptable documents at the site coordinator's discretion. For taxpayers or dependents who do not qualify for an SSN, the volunteer must review an IRS-issued ITIN card or letter or assist with applying for an ITIN. The mismatch of names and SSN or ITIN information is one of the top reasons for delays in processing electronic tax returns.

Exception for validating identity for taxpayers known to the site: The site coordinator has the discretion to grant an exception to the requirement to provide a valid form of identification and/or the requirement to provide proof of taxpayer identification number if the taxpayer is known to the site. The definition of "**known to the site**" refers only to a taxpayer

that frequently visits the same site every year for tax return preparation and is known to the site coordinator and the volunteers at the site. Just because a taxpayer's return was prepared at a site in a prior year, it does not automatically qualify as "known to the site". Only the site coordinator has the authority to approve these exceptions.

> **Example of known to the site**: Larry goes to a VITA/TCE site to have his taxes prepared. Larry specifically requests that Joe prepare his return. Joe has been preparing Larry's return for the past 4 years. Joe gets approval from the site coordinator to prepare Larry's return. The site coordinator approves the exception because he also knows Larry.
>
> **Example of *not* known to the site:** Larry goes to a VITA/TCE site to have his taxes prepared. Larry specifically requests that Joe prepare his return. Joe has been preparing Larry's return for the past 4 years. Joe requests approval from the site coordinator for an exception to prepare Larry's return. The site coordinator does not know Larry and does not approve the exception.

Partners and coordinators may maintain more stringent requirements for validating proof of identity and verifying a TIN. In addition, if there is an increase in identity theft returns at a particular site or in a particular area, IRS may require stronger requirements to deter this activity.

Signing the Tax Return

A taxpayer may sign a VITA/TCE-prepared tax return, whether a paper-filed tax return or Form 8879 for an e-filed tax return, only upon completion of these validation procedures.

- No tax return may be electronically filed unless all taxpayers sign Form 8879 giving permission to have their tax return e-filed.
- A parent or guardian of a minor child may sign Form 8879 or the tax return for the child by including the statement, "By (parent/guardian's signature), parent/guardian for minor child", in the signature section of the tax return. For additional information, see Publication 17, Your Federal Income Tax (For Individuals).
- If two taxpayers file a joint tax return, one taxpayer may sign the tax return for a missing spouse if authorized by Form 2848, Power of Attorney and Declaration of Representative, or a written statement (with the same information) but only if the missing spouse is:
  1. Unable to sign a tax return due to disease or injury (Form 2848 must be prepared in advance, while the taxpayer is able to sign), or
  2. Absent continuously from the U.S. (including Puerto Rico) for a period of at least 60 days prior to the due date of the tax return.

  Note: When a spouse signs Form 8879 under authority provided by Form 2848 or a written statement, Form 8453, U.S. Individual Income Tax Transmittal for an IRS e-file Return, must be mailed to the IRS with a copy of Form 2848 or the written statement.

- If taxpayers filing a joint tax return do not meet the above exception, both must be present at the site to validate proof of their identity and verify their TIN and then sign their tax return. They do not have to be at the site at the same time or on the same day, to do this. However, the tax return must not be e-filed, nor a copy provided to the taxpayer(s) until both signatures are secured on the tax return or on Form 8879, IRS e-file Signature Authorization.

Exception for signing the return for taxpayers **known to the site**:

- A taxpayer who is filing a joint tax return can be given permission by the site coordinator to take Form 8879 to a missing spouse to secure his or her signature if both taxpayers are known to the site. However, the tax return cannot be e-filed for the taxpayers until both signatures are secured on Form 8879.
- If they choose not to return with Form 8879, the site can prepare a paper tax return and provide two copies to the taxpayers. The volunteer must show the taxpayers where to sign their names on Form 1040 and provide the appropriate IRS processing center address for mailing.

Sharing the Information

Do not share information the taxpayer provides for tax return preparation with anyone who does not have a need to know. Individuals have a need to know if processing the information to its final disposition requires their involvement. Examples of "need to know" include sharing information for the purpose of obtaining guidance in tax return completion; electronically transmitting the return; and reviewing a tax return and source documents used to prepare the return. This includes returns submitted through the Virtual VITA/ TCE Model when a taxpayer is not present.

It is not acceptable to share information with others, even another volunteer, if the tax return preparation does not require their involvement. For instance, sharing income information, birth dates, or even the marital status of taxpayers with other volunteers, taxpayers, family, or friends as a matter of curiosity or interest, is not acceptable.

Sharing Taxpayer Information Through Virtual VITA/TCE Channels

Information sharing is normally done in-person in the VITA/TCE program. However, there may be situations where other communication channels may be more efficient in the process of preparing, completing and filing tax returns. Any process used under Virtual VITA/TCE must be documented on the Form 14446, Virtual VITA/TCE Taxpayer Consent, and signed by the taxpayer. This form is required whenever the taxpayer's tax return is completed and/or quality reviewed in a non-face-to-face environment. Please refer to Publication 5450, VITA/TCE Site Operations for the Virtual VITA/TCE Return Preparation Models that maybe utilized.

Sites must outline in detail their virtual process on Form 15272, VITA/TCE Security Plan. The territory manager or designee must approve the plan prior to implementation at the site. The volunteer must explain the virtual process to the taxpayer. Volunteers must advise the taxpayer of the risks of using virtual methods for sharing information (lost/stolen packages, accidents, information received/accessed by an unintended recipient) so they can make an informed decision about how best to proceed with the preparation of their tax return. Sites must implement reasonable controls to ensure the security of information sharing between parties.

Please refer to the list of communication channels (below) for a full list of recommended best practices designed to provide additional safeguards for the data of the taxpayers you serve:

1. US Mail:
    - Permitted to send information between sites, and between sites and taxpayers.
    - Volunteers must consider the use of certified mail when communicating with the taxpayer under the following circumstances:
        - Site is mailing personally identifiable information back to the taxpayer.
        - Site is unable to advise the taxpayer beforehand that the personally identifiable information will be mailed.
    - Taxpayers must be encouraged to use certified mail when sending information back to the site.
2. Courier (in-house or nationally/locally recognized delivery service):
    - Permitted to share information between parties.
    - Using a courier service provides additional safeguards such as package tracking and delivery confirmation.
3. Email:
    - Permitted. Both parties must consider using a supplemental program that secures the message with a password.
    - Before emailing information to taxpayers, the volunteer and taxpayer must agree on unique passwords/ identifiers to ensure the secure transmission of information between parties.
    - Volunteers must not use a public computer to send email.
    - Sensitive email messages must be deleted from the computer and/or server once they are no longer needed.

4. Telephone (Voice Communications):
    - Permitted to share information.
    - The volunteer and the taxpayer must consider using a unique password/identifier when communicating via telephone to clarify personally identifiable information the volunteer needs to prepare, review, and or submit the return.
    - The volunteer and taxpayer can use the same unique password/identifier combination for email transmissions (outlined in the bullet above) as with telephone communications.
    - When any call is made between the volunteer and the taxpayer, each party must share their unique password before discussions begins about the taxpayer's return or other personally identifiable information.
    - If the taxpayer cannot provide the password/identifier, it is recommended that the volunteer must inform the taxpayer that the call cannot continue, ask the taxpayer to locate the correct password, and courteously disconnect the call.
    - If the taxpayer cannot subsequently locate their password/identifier, it is recommended that they return to the site to provide the necessary information to complete the return preparation process.
    - If taxpayers call a volunteer site unprompted (without an authentication protocol in place), the volunteer must advise the taxpayer that they cannot discuss the taxpayer's return and that they must return to the site to resolve their issue.
5. Telephone (Text Communications):
    - Sites must not initiate contact via text.
    - If the taxpayer initiates contact via text, the site must advise the taxpayer of the risk of sharing personally identifiable information via text message. Volunteers must delete all text messages when no longer needed.
6. Fax Machine:
    - Permitted to share information.
    - Volunteers must advise taxpayers of the risks of using a public fax machine to transmit documents (data may remain in the queue while forms are being faxed).
    - The volunteer or taxpayer must be present to receive the fax when using a public fax machine. Individuals must be advised about the risks of transmitting documents to an unattended fax machine.
7. Video conferencing software:
    - Permitted to share information.
    - Must have a password.
    - Must have a video conferencing identification number.
    - Taxpayer must consent to use of video conferencing to share their PII.
    - Must encrypt all taxpayer data.
    - Data must not be saved or stored.
    - Partners who use this channel must consider options (such as closed captioning or chat features) that allow hearing-impaired clients to use this technology effectively. Note that there may be costs incurred for using these options.
    - Volunteers must authenticate the taxpayer's by validating the photo ID with the video picture of the taxpayer.
8. File Sharing Program:
    - Permitted to share information.
    - Partners must use a program that maintains minimally–acceptable levels of security (user authentication with password, 128-bit encryption, and audit trail capability) that monitors user activities. Partners must ensure all taxpayer data is encrypted prior to uploading and downloading in file sharing programs. Some file sharing programs charge a fee.
    - Volunteers must delete all information once tax return preparation is complete.

Taxpayer Consents

Treasury Regulations under 26 § CFR 301.7216-2 provides rules relating to the tax return preparers' use and/or disclosure of tax return information without taxpayer consent. The regulations include rules on maintaining and compiling lists for solicitation of tax return preparation services and disclosure and use of statistical compilations of data in support of their tax return preparation business.

The statute limits tax return preparers' use and disclosure of information obtained during the return preparation process to activities directly related to the preparation of the return. The regulations describe how preparers, with the informed written consent of taxpayers, may use or disclose return information for other purposes. The regulations also describe specific and limited exceptions that allow a preparer to use or disclose return information without the consent of taxpayers.

Exception: All volunteer sites using or disclosing anonymous aggregate data for fundraising, marketing, publicity, or other uses related to the volunteer sites' tax return preparation business are not required to secure the taxpayers' consent. Under the regulations, a statistical compilation is anonymous if it does not include any personally identifiable information, such as the taxpayer's name, SSN/ITIN, address or other personal information, and does not disclose cells containing data from fewer than ten tax returns. **This exception does not apply to the use or disclosure in marketing or advertising of statistical compilations containing or reflecting dollar amounts of refund, credit, or rebate, or relating to percentages.**

Tax return preparers must obtain consent from the taxpayer before using or disclosing tax return information. Sites must provide tax return preparation services regardless of the taxpayer's decision. However, the services provided may be limited to tax return preparation and tax return preparers must not use or disclose their data. Each partner must evaluate the uses of taxpayer information against IRC 7216 requirements to ensure compliance.

Relational EFINs

Electronic filing sites using relational EFINs with their tax preparation software must solicit consent to "Disclose". The relational EFIN process requires the tax preparation software provider share the return data with a third party, the primary sponsor. This sponsor must comply with IRC Sec. 7216 regulations. The taxpayer must consent to disclose their data prior to e-filing the tax return. If the taxpayer does not grant consent, or does not enter the PIN and date at a VITA or non-Tax-Aide TCE site, the site cannot e-file the return because the relational EFIN process shares the data with the preparing site and the primary sponsor at the point the return is acknowledged.

Consent Requirements

Revenue Procedure 2013-14 provides the mandatory language required in a consent to disclose or a consent to use tax return information with respect to a Form 1040-series income tax return. A taxpayer need not sign a consent to engage a tax return preparer to perform tax return preparation services if the preparer and taxpayer do not plan for the preparer to disclose or use the taxpayer's tax return information for any purpose other than preparing a return.

Partners must provide written notice to the taxpayer and receive signed consent on both notices when using or disclosing taxpayer information for purposes other than preparing tax returns (current, prior, or subsequent year), fundraising, and/or marketing activities in accordance with Treasury Regulation under IRC 7216. Both notices require taxpayer consent and must contain specific language for the particular use and disclosure.

The two types of consents are as follows:

1. Consent to “Disclose”, taxpayer information. **Disclose** means the giving out of information, either voluntarily or to be in compliance with legal regulations or workplace rules, and,
2. Consent to “Use” taxpayer information. **Use** means the act or practice of employing something.

These notices cannot be combined. They must be kept separate. Consents must meet the minimum requirements provided in 26 CFR 301.7216-3(a)(3) and must include the requirements defined in Revenue Procedure 2013-14 or its successor. The consent must:

- Identify the intended purpose of the disclosure or use.
- Identify the recipients and describe the specific authorized disclosure or use of the information.
- Identify the specific taxpayer information to be used or disclosed.
- Include the mandatory language outlined in Rev. Proc. 2013-14 or its successor.
- Include the consent duration if other than one year.
- Use 12-point type font on 8 ½ by 11-inch paper or, for an electronic consent, be in the same type as the web site’s standard text; and include the taxpayer’s signature and date.

Disclosure and use require separate consents, although multiple uses may be included in the same use consent and multiple disclosures may be included in the same disclosures consent. (Note: Multiple disclosures consents and multiple use consents must provide the taxpayer with the opportunity, within the separate written document, to affirmatively select each separate disclosure and use.)

Consent notices are valid for one year unless otherwise specified in the written notice to the taxpayer. There’s no legal requirement to retain a taxpayer’s written consent for any specified time period. Instead, return preparers must retain each signed consent for as long as needed to show the taxpayer or the government that the taxpayer consented to certain actions the partner later took. SPEC recommends partners consider maintaining signed copies of consent notices for at least three years after the disclosure and/or use of taxpayer information. Partners can maintain consent notices in paper or electronic format.

Partners must consult with their legal advisors about the risks of not maintaining consents (electronic or paper) if a taxpayer or the government brings a legal action and the partner has not printed or electronically saved its own copy of the signed consent.

During the return preparation process, the preparer must enter the taxpayer’s PIN based on the taxpayer’s preference, confirming the taxpayer’s decision. (Note: Preparers can only enter the taxpayer’s PIN on behalf of the taxpayer when the taxpayer has signed a paper consent. If the taxpayer does not sign a paper consent, the taxpayer must enter his or her own PIN in the tax preparation software if he or she is granting consent.)

If the preparer is entering the consent PIN and date into the tax preparation software the taxpayer must sign and date a paper consent form before entering the consent PIN and date into the tax preparation software when the taxpayer is granting consent. The site may give the signed paper consent form to the taxpayer or maintain it at the site. Whether the signed copy is given to the taxpayer or maintained at the site, the preparer must provide a copy of the consent in the tax preparation software with the PIN for his/her records. Note: There is no requirement the taxpayer must sign a consent if he or she is not granting consent.

Requirements for Consent to Use and Disclose Taxpayer Information

Using and Disclosing Taxpayer Information:	Requires a Consent to Use?	Requires a Consent to Disclose?	Requires a signed paper consent(s) if volunteers are entering the PIN?
Preparing current, prior, or subsequent year returns	No	No	No
Purposes other than prior, current, or subsequent year returns	Yes	Yes	Yes
Reporting the number of returns (number of types of returns such as Earned Income Tax Credit (EITC), Child Tax Credit (CTC), Prepared to use for fundraising, marketing, publicity, or other uses related to the volunteer sites tax return preparation business.	No	No	No
Reporting any data containing return dollar amounts for marketing or advertising or any other non-fundraising activities.	Yes	Yes	Yes
Reporting any data containing return dollar amounts for fundraising activities.	No	No	No
Global Carry-Forward Consents	No	Yes	Yes
Relational Electronic Filing Identification Number (EFIN) Consents	No	Yes	Yes

Mandatory Statements

Partners must include the following statements in the consents to disclose and consents to use tax return information. Select one of the following consent statements to Disclose (whichever applies) and the consent statement to Use for the taxpayer's signature.

Consent to "Disclose" (such as, financial aid, establishment of a bank account, other government agency assistance or bank products):

Required Statements:

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose your tax return information to third parties for purposes other than the preparation and filing of your tax return without your consent. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form to engage our tax return preparation services. If we obtain your signature on this form by conditioning our tax return preparation services on your consent, your consent will not be valid. If you agree

to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year from the date of signature.

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by e-mail at **complaints@tigta.treas.gov.**

Consent to "Use" (such as, financial aid, establishment of a bank account, other government agency assistance or bank products):

Required Statements:

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot use your tax return information for purposes other than the preparation and filing of your tax return without your consent.

You are not required to complete this form to engage our tax return preparation services. If we obtain your signature on this form by conditioning our tax return preparation services on your consent, your consent will not be valid. Your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year from the date of signature.

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by e-mail at **complaints@tigta.treas.gov.**

Multiple Disclosures or Multiple Uses Within a Single Consent Form:

A taxpayer may consent to multiple uses within the same written document or multiple disclosures within the same written document.

- You must provide disclosure consents and use consents in separate documents.
- Multiple disclosure consents and multiple use consents must provide the taxpayer with the opportunity, within the separate written document, to affirmatively select each separate disclosure or use.
- You must provide the taxpayer the mandatory consent language for each separate disclosure or use.
- The mandatory statements need only be stated once in a multiple disclosure or multiple use consent.

Disclosure of Entire Return:

If a consent authorizes the disclosure of a copy of the taxpayer's entire tax return or all information contained within a return, the consent must provide that the taxpayer has the ability to request limits on what tax return information is disclosed.

Refer to Publication 4396-A, Partner Resource Guide, for specific guidance on mandatory consents in the tax preparation software (including Global and Relational EFINs consents).

Maintaining Confidentiality of Taxpayer Information

VITA/TCE Security Plan

All VITA/TCE sites, except Facilitated Self Assistance (FSA) remote sites, must prepare an annual security plan to safeguard taxpayer data. Sites can use Form 15272, VITA/TCE Security Plan or a similar document which captures the same information to meet this requirement. The security plan contains two section: Section I – Security Requirements and Section II – Virtual VITA/TCE Process. All sites must complete Section I- Security Requirements which provides information on the procedures the site uses to help maintain the security of taxpayer information. Any site using a

virtual process must also complete Section II- Virtual VITA/TCE Process which must outline the entire virtual model the site uses to assist taxpayers. For additional information on the virtual models see Publication 5450, VITA/TCE Site Operations. All partners must approve the security plan. The site coordinator must sign the form and submit the form to their SPEC territory manager (or local SPEC designee) prior to opening of the site but no later than December 31.

Sites must also identify the type of equipment and the total count of each type used to support the VITA/TCE program. This includes partner owned, IRS owned, and volunteer owned equipment. There is an equipment inventory form Exhibit 4 in this document that sites can use to track all equipment the site uses.

The local territory office must approve the security plan before the site opens and forward an approved copy to the site. Sites and the territory office must maintain a (physical or electronic) copy of the SPEC approved security plan. Volunteers must be familiar with the security plan policies to keep taxpayer information secure and confidential.

Protecting Physical and Electronic Data

Technology comes with inherent risks. IRS and, if applicable, local governments require e-file sites to maintain certain taxpayer information. These requirements pertain to both electronic and printed data. This requirement increases the responsibility of all volunteers and partners to be vigilant in safeguarding the information. Protection involves the physical protection of the equipment used, as well as the protection of the electronic data. Partners and volunteers must protect physical and electronic data gathered for tax return preparation both during and after the filing season.

Volunteers and sponsors must protect individual information during return preparation and once the tax return is complete. Protecting the information is not limited to preventing theft but to ensuring the information is recoverable. If on-line tax preparation software is not used, partners must regularly make backup copies of the data they process in the event of computer failure. The tax software provided by IRS for tax preparation automatically encrypts tax data whether it is stored on the user's computer or on removable media. This action reduces the chance that the taxpayer could be harmed by the inability to file a return.

Partners and volunteers must take the following steps to protect both printed and electronic data when using the methods below to retain taxpayer data.

- **Printed Media** – Secure printed documents containing taxpayer information during and after operating hours.
    - Ensure Forms 8879 and 13614-C, along with any related information, is not inadvertently revealed to others. There is no requirement for VITA/TCE volunteers to retain Form 8879, IRS e-file Signature Authorization and supporting documents such as Form 13614-C, Form W-2 and Form 1099. The taxpayer(s) must sign and date Form 8879, after reviewing the return and confirming the information is accurate. The volunteer must return the signed Form 8879 to the taxpayer along with a copy of their tax return. Forms 8879 are not sent to the IRS.
    - Store paper documents away from the flow of traffic, and out of the reach of clients who may inadvertently retrieve these documents with their own papers.
    - Protect reports showing Submission ID Numbers and e-file Acknowledgments. Note: Any sensitive information not returned to the taxpayer or authorized by the taxpayer to be kept for retention by the site, must be shredded or burned when no longer needed.
    - Ensure volunteers do not maintain copies of tax returns (electronic or paper) and any related information unless it complies with IRC 7216 or return retention guidelines outlined in Publication 1345, Handbook for Authorized IRS e-file Providers of Individual Income Tax Returns.
- **Stored Data –** Take basic steps to protect data stored on your systems. Use drive encryption to lock files and all devices including mobile devices; encrypted files require a password to open.
    - Avoid attaching USB drives and external drives with client data to public computers.

- Avoid installing unnecessary software or applications to the business network; avoid offers for “free” software, especially security software, which is often a ruse by criminals; download software or applications only from official sites.
- Perform an inventory of devices that store client tax data, i.e., laptops, smart phones, tablets, external hard drives, etc.; inventory software used to process or send tax data, i.e., operating systems, browsers, applications, tax software, web sites, etc.
- Limit or disable internet access capabilities for devices that have stored taxpayer data.
- Delete all information from devices, hard drives, USBs (flash drives), printers, tablets or phones before disposing of devices; some security software include a “shredder” that electronically destroys stored files.

- **Portable Mass Storage Devices (PMSD)** – Encrypt and protect PMSD, such as external hard drives (CDs, DVDs, USBs) or cloud storage.
  - Place identification labels on the PMSD and establish a system to control and account for them.
  - Store devices in a secure location to prevent theft/loss of information. If using the cloud, encrypt the data before uploading.
  - Destroy hard drives, tapes, USBs, CDs, tablets or phones by crushing, shredding or burning; shred or burn all documents containing taxpayer information before throwing away.
- **Electronic Information Stored on Computers** – Taxpayer information stored on computers may be subject to unauthorized access. The ERO should work with the site coordinator to ensure every possible precaution is in place to protect taxpayer information and privacy. Desktop software encrypts data stored in Desktop; however, the same precautionary measures must be taken regardless of which software is used.
  - Use antivirus and firewall software on all computers used for tax preparation and when connecting to the Internet to prevent unauthorized access.
  - Use of online software requires that online providers follow the six security and privacy standards in Publication 1345; however, below are some general steps for staying safe while using the Internet to access your Online software.
    - Keep your web browser software up to date so that it has the latest security features. If your browser homepage changes, it could be a sign of malware or an intrusion.
    - Scan files using your security software before downloading to your computer.
    - Delete web browser cache, temporary internet files, cookies and browsing history on a regular schedule.
    - Look for the “S” in “HTTPS” connections for Uniform Resource Locator (URL) web addresses. The “S” stands for secure, e.g., **www.irs.gov**.
    - Avoid accessing emails or information from public wi-fi connections.
    - Disable stored password feature offered by some operating systems.
    - Enable your browser’s pop-up blocker. Do not call any number from pop-ups claiming your computer has a virus or click on tools claiming to delete viruses.
    - Do not download files, software or applications from unknown websites.
- **Networking Desktop Software** - We strongly encourage partners to use IRS loaned computers when using desktop software to protect taxpayer PII. Using LANs at sites is also recommended. A sub-network with its own router creates a secure system, separate from your site host’s computers and simplifies printer setup. Using a LAN for Desktop software also has numerous advantages especially for the e-file site manager, as listed below:
  - Only one computer holds the data;
  - Only one computer requires Desktop updates;

- Only one computer needs to be backed up;
- All networked computers have access to all returns when the network is running;
- Quality Review can be conducted from any one of the networked workstations;
- Printer sharing is easy as printer switches are not required. NOTE: When using network printers, always set them up with a "static IP address" to ensure the printer will not be "lost" by the network when a router can randomly reassign IP addresses each time the network is setup.

- **File Sharing** – Peer-to-peer (P2P) file sharing is a popular way to exchange or "share" files. Any software or system allowing individual users of the Internet to connect to each other and trade files is considered P2P. This includes applications that allow users to immediately communicate with each other via instant messaging and those that allow multiple computers to pool their processing power and memory to create a supercomputer. Before using P2P file sharing ensure you understand the risks. P2P software causes problems that may not be fully understood. Some files can be made public using this software. Therefore, all volunteers must properly protect non-IRS computers. Use of P2P applications introduce security risks, such as:
    - Exposing data/system to viruses/malicious code;
    - Placing personal and/or sensitive information at risk of unauthorized access;
    - Imposing capacity constraints on computers and networks.
- **Encryption Software** – Desktop and Online software encrypts all taxpayer information; the use of separate encryption software is not necessary. Each partner needs to self-assess the risk to determine if they will continue to use encryption software on the computer hard drives used for tax return preparation. The IRS loaned computers will continue to use encryption software to protect the whole disk on these computers as required by current government policy.

Minimum Security Practices for Safeguarding Taxpayer Data

Partners and volunteers must implement a process that protects the taxpayer's information. The process must include:

- **Securing taxpayer data on computer systems**
    - Position computer screens so unauthorized individuals cannot see taxpayer information.
    - Require computers which store taxpayer information be password protected to prevent unauthorized access. The ERO must work with the Site Coordinator and/or volunteers to develop a system that uses strong passwords. Volunteer must change their passwords periodically (at a minimum, every 90 days) or as required to protect taxpayer information. Desktop software requires the use of a strong password. A strong password must:
        - Include at least 8 characters and include numbers or symbols. The longer the password, the tougher it is to compromise.
        - Avoid common words - some hackers use programs that can try every word in the dictionary.
        - Not use personal information, your login name, or adjacent keys on the keyboard as passwords.
    - Do not post the passwords on or near equipment or in a laptop case.
    - Do not put passwords in an automatic script routine or program.
    - Each user must have a unique username and unique password. Administrator passwords must be unique and only known to select Admin level users. Partners must have a process in place to identify every volunteer that prepares or make changes to every tax return.
    - Multi-factor authentication (MFA) should be used whenever there is an option. An example of two-factor authentication requires your username and password plus a security code sent as a text to your mobile phone before you can access an account. IRS tax preparation software currently uses (MFA). It is a requirement for ALL professional web-based software providers.
    - Sign off and lock equipment when not in use. Use screen savers and automatic computer lockout after a preset period of inactivity.
    - Ensure computers and printers always remain in the control of a volunteer while in use and stored in a controlled, limited access (preferably) locked location when not in use.

- Ensure information is not accessible to general computer users that share equipment.
- Ensure computer settings do not store passwords and any other key data that could provide access to information on the computer.
- Keep devices (i.e. diskettes, CDs, flash drives, pen drives, key drives, thumb drives, etc.) containing taxpayer information secure and password protected.

- **Using tax preparation software security features**
  - Modify users' permissions, as appropriate, to ensure users only have the necessary permissions to perform their duties. To minimize security risks volunteers should not have multiple user roles in the tax software.
  - Partners using IRS provided tax preparation software are strongly encouraged to use the pre-populated security templates for both volunteer preparers and administrators. These templates were created to maximize the security of return information. Volunteer access to taxpayer data should generally be limited outside of site operating hours.
  - When volunteers quit, resign, or are no longer working at the site, the ERO or Site Coordinator must immediately deactivate their usernames.
  - The site must not use generic use names or passwords, such as "volunteer".
- **Storing and disposing of taxpayer data**
  - Ensure the information provided during tax return preparation always remain under the care of the volunteer. Documents retained after the volunteer leaves the site must be stored in locked cabinets. These documents include but are not limited to tax returns, Forms W-2, W-8 BEN, and 1099.
  - Once a site no longer needs the taxpayer's information, it must return it to the taxpayer or properly dispose of it including burning or shredding the data.
  - Dispose of all electronic media and hardware in a timely manner and make sure the data is not recoverable.
  - Delete taxpayer information stored on partner owned or IRS loaned equipment once the filing season activities are completed as indicated in the site closing activities. Follow procedures to delete data shown in Publication 4473, Computer Loan Program - Welcome Package.
- **Use of secure wireless networks**
  - Partners and volunteers should use security protected wired connections when transmitting taxpayer information via the Internet. If partners/volunteers, after conducting a comprehensive risk assessment, decide to use wireless devices to transmit taxpayer information to the tax preparation software provider, they must ensure that only an encrypted password protected wireless network is used. The use of unprotected public wireless networks is prohibited. At a minimum partners and volunteers should use:
    1. Wi-Fi Protected Access-2 (WPA2) certified equipment and software. WPA2 uses government strength encryption in the Advanced Encryption Standard (AES).
    2. AES with a minimum of 256-bit encryption.
    3. WPA2 Robust Security Network (RSN) framework must be used with authentication to establish a secure wireless connection between WLAN (Wi-Fi Local Area Networks) devices.
    4. The default SSID (Service Set Identifier) must not be used. The SSID character string must not reflect names associated with VITA, TCE, IRS, or tax preparation.
    5. If using unknown networks or working from home, partners and volunteers are strongly encouraged to establish an encrypted Virtual Private Network (VPN) to allow for a more secure connection. A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the internet and the company network.
  - Partners and volunteers are encouraged to use the tax preparation software provider's online system that stores all taxpayer data on a secure server located within the tax preparation software provider's data center.

- Partners and volunteers must exercise caution and properly safeguard the taxpayer's return and personal information. Partners and volunteers must have sufficient knowledge of the equipment (computer, software, routers, and wireless devices) they use to adequately assess their security risks and take reasonable steps to mitigate those risks.

- **Recognizing Phishing Scams**
  - Partners and volunteers must be educated on the dangers of phishing scams. These scams can result in cybercriminals taking over your computer or accounts to steal client data. The thief may pose as your tax software provider, your data storage provider, the IRS or even a prospective client.
  - Phishing emails sometimes have an urgent subject line such as "your account password has expired". The objective is to entice you to open a link or an attachment.
    - The link may take you to a fake site made to appear like a trusted source to steal your username and/or password.
    - The attachment may contain malware, which secretly downloads and allows thieves to eventually steal all the tax preparers passwords.
  - Create "trusted customer" policies; contacting potential clients by phone or video conference.
  - Do not respond to suspicious or unknown emails.

Reporting Data Breaches

A VITA/TCE data breach occurs when a taxpayer's personally identifiable information (PII) is shared, used or disclosed, whether physical or electronic, without taxpayer permission. There are two types of data breaches:

a) Unintentional (a mistake) – volunteer mistakenly provided a copy of another taxpayer's tax return or tax documents in error.

b) Intentional (on purpose) – data loss incidents such as accessing a volunteer preparer network without permission and/or theft of PII.

When a potential data breach occurs, (unintentional or intentional) partners must contact their local SPEC Territory Office immediately upon confirmation of the incident. The territory office must review the details of the incident and determine if it meets the criteria of a potential data breach. If determined to be a potential data breach, partners must provide the following information:

- Date the incident occurred
- Brief description of the data breach
- Full name and telephone number for the point of contact who reported the data breach
- Partner name and address
- Site name and address

The local SPEC territory will work with headquarters to determine if the potential data breach must be forwarded immediately to the IRS Returns Integrity and Compliance Service (RICS) data loss mailbox. If forwarded to RICS data loss mailbox, a member from the IRS RICS team will contact you to discuss the potential data breach and obtain the partner client list and any other breached items. The information requested is based on the specifics of the data breach but could include SSNs EFINs, PTINs, etc. Do not submit any taxpayer information to SPEC.

In addition, partners must also report data breaches to the following:

- Local police – File a police report on the breach
- States – Contact states in which you prepare state returns:
  - Email the Federation of Tax Administrators at **StateAlert@taxadmin.org** to get information on how to report victims.

- State Attorneys General for each state in which you prepare returns. Most states required the attorney general be notified of data breaches.

Note: For a complete checklist, refer to **Data Theft Information for Tax professionals**.

Reporting Stolen and Lost Equipment

Unfortunately, a few partners report incidents of lost or stolen computers and printers each year. Please remember these safeguarding rules to prevent a loss:

- Do not leave the laptop or printer in a vehicle where it is visible. When transporting equipment, place in the trunk or under cover on the floor of the vehicle.
- Do not store the laptop or printer in a vehicle; use vehicles for transporting only.
- Do not leave the laptop or printer unattended in a public location.
- Do not leave the laptop or printer in a closet or cabinet that does not lock and where access is not limited.
- Record the make, model and serial number of all computer equipment used and keep in a secure location. This can save valuable time if it is necessary to report the equipment as lost or stolen.

With heightened attention on security of data and computers used in support of the volunteer program, partners and volunteers must report all incidents of stolen and lost equipment (including partner owned) to the IRS.

As a condition of IRS-loaned equipment, the recipient agrees to immediately notify IRS of IRS loaned equipment **(computers and printers)** that is stolen or lost, but not later than the next business day after confirmation of the incident. Partners must immediately notify IRS, but not later than the next business day after confirmation of the incident, if a partner owned **computer** is stolen or lost. If the lost or stolen equipment contained taxpayer PII data, the partner must report the loss of PII data based on data breach guidance.

Partners much provide what is readily available to their local relationship manager or territory office. The territory office must complete an incident assessment and supporting documentations within ten days. To assist IRS with documentation, partners must provide the following:

- Serial number
- Barcode
- Make
- Model of computer or printer
- Description of what occurred
- Taxpayer data that is at risk (include number of records)
- Whether the computer was encrypted
- If not encrypted, did the computer have a strong password
- Whether the taxpayer was or will be notified of theft/loss (if notified, method used)
- A copy of police report filed with local law enforcement (if applicable)

Stolen and Lost Information – Taxpayer Notification

No matter how partners and volunteers diligently protect taxpayer information, there is always a chance that it will be stolen or lost. If this occurs, notify the appropriate authorities and then thoroughly evaluate the incident. Be sure to take action to prevent other losses of equipment. Because each incident of loss is unique, partners must evaluate the circumstances surrounding the loss and decide whether the risk of identity theft warrants notification of the individuals whose information may have been compromised.

The following table depicts situations that have occurred and will prove helpful in evaluating risk and determining whether the partner must consider notifying the taxpayer. All examples assume that individual tax return information is present.

Situation	Risk Assessment
Someone stole a laptop and bag including a note card with the passwords to the computer programs.	High risk because of the accessibility of the password in the computer bag.
The volunteer discovers someone stole their laptop but not the passwords to access the programs on the computer. The software program (Desktop and Online) volunteers use to prepare returns encrypts the data and only the software stores return information.	High Risk because the use of passwords and encryption greatly reduces the risk of compromising the taxpayer's data.
An angry taxpayer stole a folder with information reports (Forms W-2, 1099) and Forms 8879.	High risk because of the ease of accessibility of the taxpayer information in the folder.
The volunteer lost a disk containing tax return information. The tax preparation software which the volunteer uses encrypts the data while saving it to the disk.	Low risk because the use of encryption on the disk greatly reduces the risk of compromising the taxpayer's data.
Someone stole the laptop and briefcase but not the password. The computer contains encryption and the briefcase contains a return acknowledgment report for accepted returns.	High risk because of the ease of accessibility of the information on the return acknowledgment report.

Protection of Partner/Volunteer Information

Partners and site coordinators must keep confidential any personal volunteer information provided.

Volunteer information is available to IRS employees for the purposes of administering the volunteer tax return preparation program. Information pertaining to a potential volunteer, such as the name, home address, phone number, photo, foreign language skill and other pertinent information may be provided to a partner for purposes of ensuring that the potential volunteer is provided an opportunity to participate in the program. Similar information pertaining to current volunteers may also be provided to a partner to help coordinate maximum efficient use of volunteer skills. Partners and volunteers must keep volunteer information confidential and must not disclose their information to unauthorized individuals.

Release of Partner Information

IRS will protect the information provided to the extent allowable by law. However, in some situations, IRS may be compelled to provide information requested under 5 U.S.C. 552, Freedom of Information Act (FOIA). For example, a FOIA request for copies of the Form 8633, Application to Participate in the IRS E-file Program, could require the release of the applicant's name, business address and whether the applicant is licensed or bonded in accordance with state or local requirements. IRS cannot control how the requester uses the information provided through a FOIA request.

Volunteer Standards of Conduct

To maintain the greatest degree of public trust in VITA/TCE Programs, all volunteers, whether paid or unpaid, must complete Volunteer Standards of Conduct certification requirements and sign Form 13615, Volunteer Standards of Conduct Agreement, prior to working at a VITA/TCE site. Partners or site coordinators must validate the volunteers' identity

using only government-issued identification prior to participation in the Volunteer Program. Refer to Publication 4961, Volunteer Standards of Conduct – Ethics Training, for complete details.

Potential Consequences of Noncompliance

The Volunteer Protection Act of 1997 excludes conduct that is willful or criminal, grossly negligent, or reckless, or conduct that constitutes a conscious, flagrant indifference to the rights or safety of the individual harmed by the volunteer. If a volunteer discloses information, fails to protect personal information or is otherwise flagrantly irresponsible with information entrusted to him/her, criminal charges or a civil lawsuit could be brought against the volunteer. Disclosure of confidential information can result in fines or imprisonment.

Another potential consequence of failure to adequately protect taxpayer information is that the IRS may discontinue the relationship with the partner or volunteer. Federal financial assistance may no longer be provided such as software, computer equipment or electronic filing privileges.

Referring Problems

In general, the site coordinator is the first point of contact for resolving any problems you encounter. If you feel you cannot take an issue to your site coordinator, email IRS at **WI.VolTax@irs.gov,** and/or contact your local relationship manager.

If you suspect an individual or company is violating the tax laws, you may report this activity on Form 3949-A, Information Referral. You may complete this form online at **www.irs.gov/pub/irs-pdf/f3949a.pdf.** Print the form and mail to: Internal Revenue Service, Fresno, CA, 93888.

Refer taxpayers who are victims of identity theft and that theft has affected their current federal income tax return to: Identity Theft Toll-free Hot-line at 1-800-908-4490. You may prepare returns for taxpayers who bring in their CP01A Notice or special PIN (six digit IP PIN). Include the IP PIN on the software main information page.

If a taxpayer believes that he or she has been discriminated against, a written complaint should be sent to the Department of the Treasury - Internal Revenue Service at the following:

Internal Revenue Service, Civil Rights Unit
1111 Constitution Avenue, NW, Room 2413
Washington, DC 20224
(Email complaints) **edi.civil.rights.division@irs.gov**

Refer taxpayers with account questions such as balance due notices and transcript or installment agreement requests to **www.irs.gov.** Refer federal refund inquiries to **www.irs.gov/refund**. Refer state/local refund inquiries to the appropriate revenue office.

If taxpayers come into a VITA/TCE site with a tax problem, and they have been unsuccessful in resolving their issue with the IRS, the Taxpayer Advocate Service may be able to help. The taxpayer's Local Taxpayer Advocate can offer special help to a taxpayer experiencing a significant hardship as the result of a tax problem. The taxpayer can access **www.irs.gov/advocate** for more information.

Volunteer Safety

If a volunteer is threatened by a taxpayer at any time, first contact your local police department or 911 to remove the taxpayer from the facility. In addition, the volunteer must report the incident to:

- Treasury Inspector General for Tax Administration - TIGTA 1-800-366-4484
- Local IRS territory office, and/or
- VOLTAX referral e-mail at **WI.VolTax@irs.gov**

Form 13533, Partner Sponsor Agreement

Partners must complete Form 13533, Partner Sponsor Agreement annually. The Sponsor Agreement reiterates the key principles of privacy and confidentiality. By signing this agreement, the sponsor agrees to educate and enforce the Volunteer Standards of Conduct and the Civil Rights Laws and the impact on volunteers, sites, taxpayers and the VITA/TCE Programs for not adhering to them. National and local SPEC offices must secure and maintain a signed Form 13533 for each partner. SPEC Headquarters maintains AARP Tax-Aide and the military sponsor agreements. The territory office maintains all other agreements in the partner files.

Form 13533-A, FSA Remote Sponsor Agreement

Sponsors must complete Form 13533-A, FSA Remote Sponsor Agreement annually. The FSA Remote model provides taxpayers with access to free self-prep tax software, while assistance is provided by third-party electronic means. By signing this agreement, the sponsor agrees to adhere to the volunteer standards of conduct, and provides assurances that they will not receive any compensation from the user in exchange for access through the established web portal. National and local SPEC offices must secure and maintain a signed Form 13533-A for each partner.

Form 13533-B, Trusted Partner Sponsor Agreement

Trusted Partners must complete Form 13533-B, Trusted Partner Sponsor Agreement annually. The Trusted Partner program allows organizations to assist taxpayers with no physical mailing address to receive eligible tax credit payments. By signing this sponsor agreement, the organization agrees to adhere to the volunteer standards of conduct and provides assurance they will uphold taxpayers' civil rights, maintain program integrity, and provide reasonable protection of taxpayer information. The organization further agrees they will not receive any compensation from the taxpayer in exchange for services rendered. National and local SPEC Offices must secure and maintain a signed Form 13533-B for each partner.

Statement of Assurance Concerning Civil Rights Compliance

By signing the Form 13533, Partner Sponsor Agreement, the organization agrees to comply with the following civil rights laws and assurances in consideration of and for the purpose of obtaining federal property or other federal financial assistance from the Internal Revenue Service.

1. Title VI of the Civil Rights Act of 1964 (Pub L. 88-352), as amended, which prohibits discrimination on the basis of race, color, or national origin; Section 504 of the Rehabilitation Act of 1973 (Pub L. 93-112) as amended which prohibits discrimination on the basis of disability; Title IX of the Education Amendments of 1972 (Pub L. 92-318), as amended, which prohibits discrimination on the basis of sex in education programs or activities; and the Age Discrimination Act of 1975 (Pub L. 94-135), as amended, which prohibits discrimination on the basis of age; in accordance with those laws and the implementing regulations.

As clarified by Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, national origin discrimination includes discrimination on the basis of limited English proficiency (LEP). To ensure compliance with Title VI, the "Partner" and its "Sub-Recipients" must take reasonable steps to ensure that LEP persons have meaningful access to its programs in accordance with Department of Treasury implementing regulations and Department of Justice LEP Policy Guidance. Meaningful access may entail providing language assistance services, including oral interpretation and written translation, where necessary. The Partner and its Sub-Recipients are encouraged to consider the need for language services for LEP persons served or encountered when developing budgets and in conducting programs and activities. Resources on language assistance and information regarding LEP obligations may be found at **lep.gov** or by contacting the IRS Civil Rights Unit.

2. The Partner will conduct its activities so that no person is excluded from participation in, is denied the benefits of, or is subject to discrimination, as prohibited by the statutes identified in paragraph 1, in the distribution of services and/or benefits provided under this federal financial assistance program.

3. To compile and submit information to the Internal Revenue Service (IRS) Civil Rights Unit concerning its compliance with Title VI of the Civil Rights Act of 1964 (Pub L. 88-352), as amended, Section 504 of the Rehabilitation Act of 1973 (Pub L. 93-112), as amended, Title IX of the Education Amendments of 1972 (Pub L. 92-318), as amended, and the Age Discrimination Act of 1975 (Pub L.94-135), as amended, in accordance with those laws and the implementing regulations. All civil rights assurances signed by partners will be maintained by the IRS. Civil rights assurances signed by sub-recipients will be maintained by partners.

4. Within 30 days of any finding issued by a federal or state court or by a federal or state administrative agency that the "Partner" has discriminated on the basis of race, color, national origin (including limited English proficiency), disability, sex (in education programs or activities), or age in the delivery of its services or benefits, a copy of such finding shall be forwarded to the following:

   Internal Revenue Service Civil Rights Unit
   1111 Constitution Avenue, NW, Room 2413
   Washington, D.C. 20224
   edi.civil.rights.division@irs.gov

5. To inform the public that persons who believe they have been discriminated against on the basis of race, color, national origin (including limited English proficiency), disability, sex (in education programs or activities), or age, in the distribution of services and benefits resulting from this federal financial assistance program may file a complaint with the Civil Rights Unit, at the above address. Civil Rights posters indicating the process for filing complaints of discrimination for the public must be conspicuously displayed at all times at each "Partner's" location, as well as by its sub-recipients.

6. To forward to the Civil Rights Unit for investigation, all complaints of discrimination filed by the public against the "Partner" that is directly related to the services and/or benefits provided by this IRS federal financial assistance program.

Statement of Assurance Filing Requirement

A signed Form 13533, Partner Sponsor Agreement, is required annually from partners and its sub-recipients receiving federal financial assistance. Partners and its sub-recipients receiving federal financial assistance must comply with this assurance for one year from the date of signing the Form 13533, Partner Sponsor Agreement.

The organizational official whose signature appears on the Form 13533, Partner Sponsor Agreement, is authorized to sign this assurance and commit the "Partner" to the above provisions. The partner and sub-recipients, its successors, transferees and assignees, upon the breach or violation of this agreement, the IRS may, at its option: a) Terminate or refuse to render or continue federal financial assistance for the aid of the property, facility, project, service, or activity, b) Enforce this agreement by suit for specific performance or by any other available remedy under the laws of the United States or the state in which the breach or violation occurs.

Data Collection Requirements

Currently, recipients of federal financial assistance from the Department of the Treasury must meet certain legal requirements relating to nondiscrimination and nondiscriminatory use of federal funds. Those requirements include ensuring entities receiving federal financial assistance from the Treasury do not deny benefits or services, or otherwise discriminate on the basis of race, color, national origin, disability, and age, or on the basis of sex in educational programs and activities. The Department of the Treasury has an obligation to enforce nondiscrimination requirements to ensure the administration of federally-assisted programs and activities in a nondiscriminatory manner. In order to carry out its enforcement responsibilities, the Department must obtain a signed assurance of compliance and collect and review information from recipients to determine their compliance with applicable requirements before and after providing financial assistance (see 31 CFR 22.5, 22.6 and 28 CFR 42.406).

In accordance with the Title VI regulations (see 31 CFR 22), the Department of the Treasury is authorized to request data from its recipients and those applying to receive financial assistance from the Department. Treasury will request recipients to submit a Title VI narrative describing their compliance status at the time of the application for assistance. The Department will also request recipients to submit data during post-award compliance reviews. Please note that Treasury and/or its bureau will make available sample policies and procedures to assist recipients in completing these requests for data, and will provide technical assistance directly to recipients as needed.

The purpose of the information collection is to advise recipients of their civil rights obligation; obtain an assurance of compliance from each recipient, and collect pertinent civil rights information to determine if the recipient has adequate policies and procedures in place to achieve compliance, and determine what, if any, further action may be needed (technical assistance, training, compliance review, etc.), to ensure the recipient is in compliance and will carry out its programs and activities in a nondiscriminatory manner. Treasury will also collect civil rights related information from all primary recipients of federal financial assistance from the Department. Primary recipients are non-federal entities that receive federal financial assistance in the form of a grant, cooperative agreement, or other type of financial assistance directly from the Department and not through another recipient or “pass-through” entity. Please note that this information collection does not apply to sub-recipients, federal contractors (unless the contract includes the provision of financial assistance), nor the ultimate beneficiaries of services, financial aid, or other benefits from the Department.

Many recipients already collect information, including race and national origin data, on the beneficiaries that receive tax preparation assistance. Recipients must provide information with their application for federal financial assistance. Treasury anticipates that data, records or files used to respond to the information collections are already maintained in electronic format by the recipient, so providing the information electronically will further minimize administrative burden. Treasury will also allow recipients to scan and submit documents not maintained electronically. Recipients must make alternate arrangements to submit hard copy if they cannot submit their information electronically.

Recipients can submit comments to the Office of Equity, Diversity and Inclusion, Civil Rights Unit concerning data collection for civil rights compliance and enforcement purposes under Title VI of the Civil Rights Act, and similar statutes applicable to Federal financial assistance, by emailing **edi.civil.rights.division@irs.gov**.

Reference Materials

For further information and guidance, please refer to the following:

- **Publication 1345** – Handbook for Authorized IRS e-file Providers
- **Publication 1084** – Volunteer Site Coordinator’s Handbook
- **Publication 4396-A** – Partner Resource Guide
- **Publication 4473** – Computer Loan Program Welcome Package
- **Publication 4557** – Safeguarding Taxpayer Data
- **Publication 5027** – Identity Theft Information for Taxpayers

Exhibit 1

Form **13533** (September 2020)	Department of the Treasury - Internal Revenue Service **VITA/TCE Partner Sponsor Agreement**

We appreciate your willingness and commitment to serve as a sponsor in the Volunteer Income Tax Assistance (VITA) or Tax Counseling for the Elderly (TCE) volunteer tax return preparation programs.

To uphold taxpayers' civil rights, maintain program integrity and provide for reasonable protection of information provided by the taxpayers serviced through the VITA/TCE Programs, it is essential that partners and volunteers adhere to the strictest standards of ethical conduct and the following key principles be followed.

- Partners and volunteers must keep confidential the information provided for tax return preparation.
- Partners and volunteers must protect physical and electronic data gathered for tax return preparation both during and after filing season.
- Partners using or disclosing taxpayer data for purposes other than current, prior, or subsequent year tax return preparation must secure the taxpayer's consent to use or disclose their data.
- Partners and volunteers must delete taxpayer information on all computers (both partner owned and IRS loaned) after filing season tax return preparation activities are completed.
- Partners and site coordinators are expected to keep confidential any personal volunteer information provided.
- Partners will educate and enforce the Volunteer Standards of Conduct and Civil Rights Laws and the impact on volunteers, sites, taxpayers and the VITA/TCE Programs for not adhering to them.

1. Sponsor name

2. Street address

3. City	4. State	5. Zip code

6. Telephone number	7. E-mail address

Please review this form and Form 13615, Volunteer Standards of Conduct. By signing and dating this form, you are agreeing:

a) To the key principles,

b) All volunteers participating in your return preparation site will complete the volunteer standards of conduct training, and

c) All volunteers will agree to the Volunteer Standards of Conduct by signing and dating Form 13615.

d) To read, understand and follow the Statement of Assurance Concerning Civil Rights Compliance listed in Publication 4299, Privacy, Confidentiality and Civil Rights.

e) Form 13615 will be validated and signed by a partner designated official (Site Coordinator, partner, instructor or IRS contact).

The IRS may terminate this agreement and add you to a volunteer registry, effective immediately for disreputable conduct that could impact taxpayers' confidence in any VITA/TCE Programs operated by you or your coalition members.

Sponsor signature _____ Date _____

Print name _____

Title _____

Privacy Act Notice

The Privacy Act of 1974 requires that when we ask for information we tell you our legal right to ask for the information, why we are asking for it, and how it will be used. We must also tell you what could happen if we do not receive it, and whether your response is voluntary, required to obtain a benefit, or mandatory. Our legal right to ask for information is 5 U.S.C. 301.

We are asking for this information to assist us in contacting you relative to your interest and/or participation in the IRS volunteer income tax preparation and outreach programs. The information you provide may be furnished to others who coordinate activities and staffing at volunteer return preparation sites or outreach activities. The information may also be used to establish effective controls, send correspondence and recognize volunteers.

Your response is voluntary. However, if you do not provide the requested information, the IRS may not be able to use your assistance in these programs.

Exhibit 2

Form **13533-A**
(October 2021)

Department of the Treasury - Internal Revenue Service

FSA Remote Sponsor Agreement

We appreciate your willingness and commitment to serve as a sponsor of a Facilitated Self Assistance (FSA) Remote site, by promoting web link(s) to a third-party provider offering free online tax preparation services to taxpayers.

This Remote Sponsor Agreement must only be completed if you are not required to complete the Form 13533. This form only covers partners who are supporting remote Facilitated Self Assistance web links, and not any other VITA/ TCE tax assistance programs, either separately or together with FSA Remote.

To maintain program integrity and provide for reasonable protection of information provided by the taxpayers serviced through the FSA Program, it is essential that partners adhere to the following key principles:

- Partner agrees not to connect the promotion of the above referenced web link(s) with any request for compensation or donation from the user.
- Partner agrees to offer IRS-certified volunteer support to taxpayers who have tax law-related questions. This can occur either directly through that organization's volunteers, or by referring taxpayers to another partner/resource that can supply that service within a reasonable time-frame (usually 48 hours).
- Partner agrees to connect taxpayers to IRS VolTax (Publication 4836) and Civil Rights (Publication 4053) guidance.
- Partner agrees to refer any taxpayer questions about the FSA Program back to the third-party provider website for resolution.
- Partner agrees to follow any SPEC guidance on sharing the vendor link(s) with taxpayers to ensure the integrity of the FSA program, and to work with their Relationship Manager to resolve any issues that arise from the posting, distribution and/or use of the vendor link(s).
- Partner agrees not to engage in criminal, infamous, dishonest, notoriously disgraceful conduct, or other conduct deemed to have a negative effect on the FSA Program.

1. Sponsor name			
2. Street address	3. City	4. State	5. ZIP code
6. Telephone number	7. Email address		

By signing and dating this form, you are agreeing to the key principles outlined above.

Website(s) where FSA link will be located *(if more space is needed, list the additional websites on a separate document)*

The IRS may terminate this agreement and add you to a volunteer registry, effective immediately for disreputable conduct that could impact taxpayers' confidence in the FSA Program operated by you or your coalition members.

Sponsor signature	Date
Name *(print)*	Title

Privacy Act Notice

The Privacy Act of 1974 requires that when we ask for information we tell you our legal right to ask for the information, why we are asking for it, and how it will be used. We must also tell you what could happen if we do not receive it, and whether your response is voluntary, required to obtain a benefit, or mandatory. Our legal right to ask for information is 5 U.S.C. 301. We are asking for this information to assist us in contacting you relative to your interest and/or participation in the IRS volunteer income tax preparation and outreach programs. The information you provide may be furnished to others who coordinate activities and staffing at volunteer return preparation sites or outreach activities. The information may also be used to establish effective controls, send correspondence and recognize volunteers. Your response is voluntary. However, if you do not provide the requested information, the IRS may not be able to use your assistance in these programs.

Exhibit 3

Form **15272** (October 2021)	Department of the Treasury - Internal Revenue Service **VITA/TCE Security Plan**

Purpose: This form provides information on the procedures used at the VITA/TCE site location to help maintain the security of taxpayer information and adherence to the security requirements outlined in Publication 4299, Privacy, Confidentiality, and Civil Rights – A Public Trust. In addition, it also provides information on any Virtual VITA/TCE Models the site uses to assist taxpayers and if the site adheres to all Quality Site Requirements outlined in Publication 5166, VITA/TCE Quality Site Requirements.

Directions: All sites (excluding FSA remote sites) must complete Section I- Security Requirements of this form. Any site using a virtual process must also complete Section II-Virtual VITA/TCE Model. The site coordinator must sign the form. Sites must submit this form for approval to their SPEC territory manager (or local SPEC designee) prior to the site opening but no later than December 31. Sites can use this form or a similar document that captures the same information to meet this requirement. Sites and the territory office must maintain a (physical or electronic) copy of the SPEC approved security plan.

Site name	Site address

Partner name	EFIN	SIDN

Type of software used

☐ TaxSlayer online ☐ TaxSlayer desktop ☐ Other *(list name)* _____

Date completed	Completed by

Role	Name	Telephone Number	Email Address
Site Coordinator			
Alternate Site Coordinator			

Complete equipment inventory log. Identify the type of equipment and the number used to support the site. Include only IRS owned, partner owned, and volunteer owned equipment.

Type of Equipment	# IRS Owned	# Partner Owned	# Volunteer Owned
Laptops			
Portable mass storage devices *(ex. CD, DVD, or USB)*			
Other *(ex. tablets, printers, smartphones, etc.)*			

Section I - Security Requirements

Refer to Publication 4299, Privacy, Confidentiality, and Civil Rights – A Public Trust, that outlines the security requirements for questions 1 through 9. At the end of each question, the section and page number is listed for additional information.

1. Are procedures in place at the site to confirm volunteer awareness 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. ***Refer to Privacy and Confidentiality – Key Principles - Page 2*** ☐ Yes ☐ No

2. If using a wireless network at the site, are volunteers following the requirements in Publication 4299 to restrict unauthorized access to the site's wireless network? If no, explain. ***Refer to Use of secure wireless networks - Page 14*** ☐ 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. ***Refer to Utilizing tax preparation software security features - Page 14*** ☐ Yes ☐ No

Exhibit 3

4. Are volunteers following security requirements 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. ***Refer to Portable Mass Storage Devices/Electronic information Stored on Computers - Page 12*** ☐ 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. ***Refer to Privacy During the Interview - Page 3*** ☐ 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. ***Refer to Utilizing tax preparation software security features - Page 14*** ☐ Yes ☐ No

7. Is the site coordinator aware of the process for reporting a 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. ***Refer to Reporting Stolen and Lost Equipment - Page 16*** ☐ 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. ***Refer to Reporting Data Breaches – Page 15*** ☐ Yes ☐ No

9. Are volunteers properly securing ((physical and or electronic) taxpayer Personally Identifiable Information (PII) in their possession and disposing of the information when no longer needed? If no, explain. ***Refer to Protecting Physical and Electronic Data - Page 11*** ☐ 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. Does the site coordinator follow the guidelines in Publication 1084, *VITA/TCE Site Coordinator Handbook*, for closing the site? If no, explain ☐ Yes ☐ No

12. Does the site plan to use a Virtual VITA/TCE Model to assist taxpayer's with tax preparation? If yes, complete Section II Virtual VITA/TCE Process. If no, skip to Part III. ***Refer to*** Publication 5450***, VITA/TCE Site Operations*** ☐ Yes ☐ No

Exhibit 3

Section II - Virtual VITA/TCE Process

Part I - Virtual Model and Site Information

Select the Virtual VITA/TCE Model from the drop-down menu. Refer to Publication 5450, VITA/TCE Site Operations for a description of the virtual models.

Virtual VITA/TCE model

Part II - Virtual Process

Describe in detail how the site remotely performs each virtual return preparation process. If the site performs any of the virtual processes listed at the site directly with the taxpayer, indicate N/A by the appropriate question. Refer to Publication 5450, VITA/TCE Site Operations for more information.

1. Describe the sites appointment scheduling process *(if applicable)*

2. Describe the process for securing Form 14446, Virtual VITA/TCE Taxpayer Consent

3. Describe the sites intake process. List the documents the site requires during intake and how they receive documents at this stage of the process

4. Describe the process to authenticate the taxpayer and the spouse. Address the video conferencing or file sharing systems the site uses and the documents they review

5. Describe the site interview process

6. Describe the sites virtual tax return preparation process

7. Describe the site quality review process

8. Describe the site process for sharing the completed return for the taxpayer to review and sign

9. If the original source documents are dropped off, how does the site secure, return and dispose of the documents after use

Exhibit 3

10. Describe the process and timeframe for transmitting returns and working rejects

Part III - Disclaimers

IRS/SPEC does not endorse any specific data-sharing service. VITA/TCE sites should select the vendor and/or product that best meets the partner's needs as determined by their own organization's information technology support function or chief information officer.

By signing this form you are approving the security requirements and virtual processes used by the site.

Approver's signatures

Site Coordinator name	Signature *(electronic)* **OR**	Signature *(type/print)*	Date
Relationship Manager's name	Signature *(electronic)* **OR**	Signature *(type/print)*	Date
Territory Manager's name *(or designee)*	Signature *(electronic)* **OR**	Signature *(type/print)*	Date

Exhibit 4

Equipment Inventory

***Record all computer equipment used at the site and keep in a secure location.**

	***Serial #**	***Barcode #** (if applicable)	***Make**	***Model**	***Encrypted** Yes / No	***Password Protected** Yes / No
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						