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. 9-2018) 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 provide free tax return preparation for low to moderate income and elderly taxpayers. Details governing the operation of these two programs are covered in various materials; however, one of the foundational principles for both programs is the confidentiality of taxpayer information is guaranteed so that the public trust is protected. This document addresses areas where diligence to detail is needed.

Section 7216 of the Internal Revenue Code (IRC) and a related provision, IRC 6713, provide penalties against tax return preparers 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

Partners and volunteers are not subject to the same statutes and regulations to which IRS employees are held accountable. Information provided by individual taxpayers to a VITA/TCE volunteer is not considered "return information" protected by IRC 6103 until it is received, recorded, or collected by the IRS. 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 utilizing volunteer program services provide Personally Identifiable Information (PII) to the volunteers, such as names, addresses, Social Security Numbers, 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.

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, they are still considered volunteers by the VITA/TCE Programs. To ensure protection, those who do not fit this VPA volunteer definition should 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 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. Refer to the section on IRC 7216 later in this publication for exceptions to securing the taxpayer's consent.
- 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 must keep confidential any personal volunteer information provided.

Taxpayer Information

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

Taxpayers Must Participate in Return Preparation

All tax returns should be prepared at the site with the taxpayer present unless (1) a joint return is being prepared for a married couple and one taxpayer is present at the site or (2) a return is being prepared for a minor child and the child's parent or guardian is present at the site. Otherwise, VITA/TCE sites must not prepare a tax return without the taxpayer's participation even if the taxpayer has authorized another person to represent the taxpayer for the preparation of a tax return. In addition, taxpayer information should not be dropped off at a site for tax return preparation at a later time. Please note the Exception below for Virtual VITA/TCE.

Exception: Having the taxpayer present in the preparer's site at the same moment the tax return is being prepared is not always possible. In these cases, Virtual VITA/TCE processes can be used 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 used 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 1084, Volunteer Site Coordinator Handbook, for more information on Virtual VITA/TCE processes.

In situations where a taxpayer presents information that is not sufficient to complete the return, all documents should be returned to the taxpayer with a request that they be brought back, along with the remaining information needed to complete 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. While arranging 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.

When volunteers require assistance to complete the tax return, they should ensure privacy is maintained during these discussions.

Requesting the Information

When preparing tax returns, only information that is necessary and relevant should be requested. The information provided is entrusted to the volunteer with the taxpayer's confidence that it will not be shared or used in any unauthorized manner.

Information such as name, address, Social Security Numbers (SSN), birth dates, marital status, bank account information for direct deposit, and other basic information is necessary to prepare the tax return. Documents such as government issued photo ID, employer ID, school ID, social security cards, and ITIN letters are necessary to ensure identity and accuracy.

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

The following validation procedures must be followed before a taxpayer may receive a copy of or sign a VITA/TCE prepared tax return. Typically, they should be followed prior to tax return preparation.

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. However, judgment should be used to accept 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 should be advised to return with an acceptable form of identification. Exceptions to requiring an original photo ID should 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 should 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, a Medicare card that includes the letter "A" after the SSN, 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 and/or verifying the taxpayer identification number: 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**" includes 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. However, only the site coordinator can approve these exceptions.

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 when these validation procedures are complete.

- No tax return may be electronically filed unless all taxpayers sign Form 8879 giving permission to have their VITA/TCE tax return e-filed.
- A parent or guardian of a minor child may sign Form 8879 or the tax return for the child with, "By (parent/guardian's signature), parent/guardian for minor child."
- If two taxpayers are filing 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.

- Otherwise, two taxpayers filing a joint tax return should 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 cannot 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*.

However, at the coordinator's discretion the following **exception** can be used:

1. 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. 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, a paper tax return can be prepared and two copies provided to the taxpayers. The taxpayers should be directed where to sign their names on Form 1040, and given the appropriate IRS processing center address for mailing.

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.

Partner, Site Coordinators, or IRS Discretion:

Please note that partners and coordinators may maintain more stringent requirements for validating proof of identify 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.

Sharing the Information

Information provided for tax return preparation should not be shared with anyone who does not have a need to know.

Individuals have a need to know if their involvement is required to process the information to its final disposition. 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 their involvement in the tax return preparation is not required. 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 Non-Traditional Channels

Information sharing is normally done face-to-face 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. For example:

- A volunteer needs advice from a more experienced preparer with an entry on the tax return. The more experienced preparer is offsite.

- The taxpayer's return has rejected due to a mismatch between the name and SSN on the return. The site coordinator must contact the taxpayer to obtain the corrected information needed to resolve the Reject Code.

- The taxpayer consents to any Virtual VITA/TCE process (using the Form 14446, ***Virtual VITA/TCE Site Model Taxpayer Consent***) to prepare, review, and/or submit their return. Any process utilized under Virtual VITA/TCE must be documented on the Form 14446.

In these cases, non-traditional means for sharing PII and other sensitive information may be used to accomplish this goal. These recommendations have been developed in an effort to balance the security of taxpayer information with the

potential impact on VITA/TCE partners impacted by these provisions. Volunteers and taxpayers should be advised of the risks of using non-face-to-face methods for sharing information (lost/stolen packages, accidents, information received/ accessed by an unintended recipient) so that they can make an informed decision about how best to proceed with the preparation of their tax return. Reasonable controls should be implemented to ensure the security of information sharing between parties. Please refer to the list of non-traditional 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 should 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 should 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 should consider using a supplemental program that secures the message with a password.
    - There are several software programs available for download for both partners and taxpayers. Note that although some programs are free, there are others that may charge a fee.
    - Before emailing information to taxpayers, the volunteer and taxpayer should agree on unique passwords/identifiers to ensure the secure transmission of information between parties.
    - Volunteers should not use a public computer to send email.
    - Sensitive email messages should be deleted from the computer and/or server once they are no longer needed.
4. Telephone (Voice Communications):
    - Permitted to share information.
    - As with email above, both the volunteer and the taxpayer should consider using a unique password/identifier to be used when a phone call is placed to clarify personally identifiable information needed 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 should share their unique password before discussions begins about the taxpayer's return or other personally identifiable information.
    - If a site is utilizing the recommended password/identifier protocol and the taxpayer cannot provide the password/identifier, it is recommended that the volunteer should 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 should return to the site to provide the information needed to complete the return preparation process.
    - If taxpayers call a volunteer site unprompted (without an authentication protocol in place), the volunteer should 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):

    - Not permitted to be initiated by the site.
    - If the taxpayer initiates contact via text, the site should advise the taxpayer of the risk of sharing personally identifiable information via text message.

6. Fax Machine:

    - Permitted to share information.
    - Taxpayers should be advised of the risks of using a public fax machine to transmit documents (data may remain in the queue while forms are being faxed).
    - If a public fax machine is used to receive a transmission, the volunteer or taxpayer should be present to receive the fax. Individuals should be advised about the risks of transmitting documents to an unattended fax machine.

7. Videoconferencing:

    - Permitted to share information.
    - Volunteers should not share personally identifiable information during the videoconference session (and advise the taxpayer to do likewise). If the taxpayer insists on sharing PII, the volunteer should consider discontinuing the videoconference session.
    - Partners who utilize this channel should consider options (such as closed captioning or chat features) that allow hearing-impaired clients to utilize this technology effectively. Note that there may be costs incurred for utilizing these options.

8. File Sharing Program:

    - Permitted to share information.
    - Partners should acquire a program that maintains minimally–acceptable levels of security (user authentication with password, 128-bit encryption, and audit trail capability) so that user activities can be monitored. There may be a partner cost involved.

IRC 7216 - Disclosure and Use of Taxpayer Information

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.

All volunteer sites using or disclosing taxpayer data for purposes other than preparing a current, prior, or subsequent year tax return must secure the taxpayer's consent to use and disclose the data. See Revenue Procedure 2013-14.

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 percentages relating thereto.

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 EFIN Consents	No	Yes	Yes

Tax return preparers must obtain consent to use or disclose tax return information before tax return information is used or disclosed. **Tax return preparation services must be provided regardless of the taxpayer's decision on whether to agree to the use and disclosure of their data. Taxpayers who choose not to consent to the use or disclosure of their data must not be denied services;** however, the services provided may be limited to tax return preparation and tax return preparers must not use or disclose their data. Each partner/volunteer organization must evaluate the uses of taxpayer information against IRC 7216 requirements to ensure compliance.

Consent - Requirements

Partners are required to 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 7216. Partners must customize consents to be specific for their particular use and disclosure.

There are two types of consents:

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.
- Separate consents are required for disclosure and use, 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 should retain each signed consent for as long as it may be needed to show to the taxpayer or to the government that the taxpayer consented to certain actions that 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. Consent notices may be maintained in paper or electronic format.

Partners should 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 should 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, then 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 at the site. Whether the signed copy is given to the taxpayer or maintained at the site, a copy of the consent in the tax preparation software with the PIN must be provided to the taxpayer for his/her records. Note: A taxpayer is not required to sign a consent if he or she is not granting consent.

Mandatory Statements

The following statements must be included in 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 taxpayers 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.

- Disclosure consents and use consents must be provided 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.
- The taxpayer must be provided 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).

Use of Wireless Devices in the VITA/TCE Programs

IRS recommends partners/volunteers use wired connections when transmitting taxpayer information via the Internet. If partners/volunteers, after assessing their individual risks, decide to use wireless devices to transmit taxpayer information to the tax preparation software provider, at a minimum, partners/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 should 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) should not be used. The SSID character string should not reflect names associated with VITA, TCE, IRS, or tax preparation.

Partners/volunteers are encouraged to use the tax preparation software provider's online system when using wireless devices since all taxpayer data is stored on a secure server located in the tax preparation software provider's data center.

Partners/ volunteers are expected to exercise caution to ensure taxpayer return and personal information is properly safeguarded. Partners/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.

Maintaining and Ensuring Confidentiality of Taxpayer Information

Technology comes with inherent risks. E-file sites are required by IRS and, if applicable, by local government 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.

Protecting the Information

Once the tax return is complete and the taxpayer has left, volunteers and sponsors must ensure the individual information provided during return preparation is protected. 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 should regularly make backup copies of the data they process in the event of computer failure. The 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.

Copies of tax returns (electronic or paper) or related information must not be maintained by any individual volunteer 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.*

Exception: VITA/TCE volunteers are not required 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 should return the signed Form 8879 to the taxpayer along with a copy of their tax return. Forms 8879 are not sent to the IRS.

- **Printed media** – Ensure printed documents containing taxpayer information are secured during and after operating hours. Although a locked storage area is preferred, it may not be available while on site. Care should be taken to ensure Forms 8879 and 13614-C, along with any related information, is not inadvertently revealed to others. 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. Reports showing Submission ID Numbers and e-file Acknowledgments should be protected. 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.

- **Protecting Stored Data –** Ensure basic steps are taken to protect data stored on your systems. Use drive encryption to lock files and all 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 where client tax data are stored, 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)** – PMSD, such as external hard drives (CDs, DVDs, USBs) or cloud storage must be encrypted and protected. Place identification labels on the PMSD and establish a system to control and account for them. These devices should be stored in a secure location to prevent theft/loss of information. If using the cloud, the data must be encrypted before uploading. Physically 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. Encryption is not required if only storing back-up files from the software.

- **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 should be taken regardless of which software is used. Use of antivirus and firewall software is required on all computers used for tax preparation and when connecting to the Internet to prevent unauthorized access.

  If using Online software, Online preparers also must 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.
  - 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., https://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.
  - Note if your browser homepage changes; it could be a sign of malware or an intrusion.

- **Networking Desktop Software** - Many sites are now successfully using simple Local Area Networks (LANs) for improved productivity and security. Using LANs at sites is strongly encouraged. 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:

  - Better security - only one computer actually 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 is allowed to 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 super computer. 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.
  - 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 through the use of this software. Therefore, all volunteers must ensure that non-IRS computers are properly protected.

- **Encryption Software** – Since the Desktop and Online software encrypts all taxpayer information, the use of separate Encryption Software is not necessary. Each volunteer 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.

Providing a Safe Environment for Information

Partners and volunteers must implement a process to ensure information is adequately protected at all times. The process must:

- Ensure the information provided during the course of tax return preparation is under the care of volunteers at all times and in accordance with partner security and safeguarding guidance/directives.

- Position computer screens so unauthorized individuals cannot see taxpayer information.

- Password Protection - Taxpayer information stored on computers must be password protected to ensure/ prevent unauthorized access. The ERO should work with the Site Coordinator and/or volunteers to develop a system to ensure strong passwords are used and that the passwords are changed periodically or as required to ensure taxpayer information is protected. Desktop software requires the use of a strong password.

  - A strong password should have at least 8 characters and include numbers or symbols. The longer the password, the tougher it is to compromise. A 12-character password is stronger than one with 8-characters.
  - Avoid common words - some hackers use programs that can try every word in the dictionary.
  - Don’t use your personal information, your login name, or adjacent keys on the keyboard as passwords.
  - Change your password regularly (at a minimum, every 90 days).
  - Don’t use the same password for more than one user. Each user should have a unique User Name and unique password. Administrator passwords should be unique and only known to select Admin level users.
  - 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.

- Sign off or lock equipment when not in use. Use screen savers and automatic computer lockout after a preset period of inactivity.

- Ensure information is not accessible to general computer users that share equipment. The diligent use of strong passwords will protect against unauthorized access to taxpayer information.
- Operating System Passwords – All sites using computers to prepare returns are to protect access to the operating system with a password that uses strong password configuration.
- Tax Preparer Unique User Names – All volunteers using the Desktop software are strongly encouraged to create a unique user name that is password protected. Partners must have a process in place to identify every volunteer that prepared or made changes to every tax return. This policy helps to protect the volunteer as much as it protects the taxpayer.
- The volunteer‘s access privileges should be limited to the activities necessary to perform their volunteer role. For instance, a return preparer should not be assigned administrative or super user rights.
- When the site uses “other” software to prepare returns, similar security precautions should be followed as allowed by the software.
- Modify users’ permissions, as appropriate, to ensure users only have the necessary permissions to perform their duties. When volunteers quit, resign, or are no longer working at the site, the ERO or Site Coordinator must immediately deactivate their user names.
- The site should not use generic user names or passwords, such as “volunteer”.
- The site must change the password immediately when a user leaves the program.
- Desktop “Guest” accounts must be password protected. If other software is used to electronically prepare tax returns, all user and non-user accounts, such as “guest” accounts should be password protected.
- Use locked storage for documents that must be retained after the taxpayer leaves the site. These documents include but are not limited to tax returns, Forms W-2, W-8 BEN, and 1099. Keep devices (i.e. diskettes, CDs, flash drives, pen drives, key drives, thumb drives, etc.) containing taxpayer information secure.
- Disposing of information – All electronic media and hardware should be disposed in a timely manner that ensures data is not recoverable. Contact your local SPEC Territory office for additional guidance.
- Deleting Taxpayer data – Information may not be stored on partner owned or IRS loaned equipment once the filing season activities are completed. The information on all computers (both partner owned and IRS loaned) must be deleted (securely wiped) as part of the site closing activities. Deleting the information properly will prevent unauthorized disclosure of confidential information. IRS provided software encrypts all tax return data stored on the user’s computer or on removable media.
- Ensure computers/printers are in the control of a volunteer at all times while in use and stored in a controlled, limited access (preferably) locked location when not in use.
- Unfortunately, a few computers and printers are lost or stolen 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.
    - Ensure computer settings do not store passwords and any other key information that could provide access to information on the computer.
- 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.

Backup disks containing tax return information provided to the IRS for storage are subsequently used for tax administration purposes by IRS. Based on this, the disks become “return information” protected by 26 U.S.C. 6103. At this point, they cannot be returned to a partner or volunteer for any use.

Reporting Stolen and Lost Equipment

With heightened attention on security of data and computers used in support of the volunteer program, it is necessary to ensure all incidents of stolen and lost equipment (including partner owned) are reported to the IRS.

As a condition of IRS-loaned equipment, the recipient of loaned equipment agrees to notify IRS within 48 hours if equipment is stolen or lost. Partners are also requested to notify IRS within 48 hours if partner owned equipment is stolen or lost.

Partners should 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 are asked to 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 diligent partner/volunteers are in protecting 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 should 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 may prove helpful in evaluating risk and determining whether taxpayer notification should be considered. All examples assume that individual tax return information is present.

Situation	Risk Assessment
A laptop and bag are stolen. The passwords to the computer programs were recorded on a note card in the bag.	Risk is high because the password was with the computer and makes the data easily accessible.

A laptop is stolen. Passwords are required to access the programs on the computer and they were not compromised. The software program (Desktop and Online) used to prepare returns encrypts the data and return information is only stored within this software.	Risk is low. Use of passwords and encryption greatly reduce the risk of compromised data.
A folder with information reports (Forms W-2, 1099) and/or Forms 8879 is stolen from the site by an angry taxpayer.	Risk is high because the information is easily accessible.
A disk containing return information is lost. The data on the disk was saved using a tax preparation software program that encrypts the data when saved to a disk.	Risk is low. Use of encryption on the disk greatly reduces the risk of compromised data.
A laptop is stolen with encryption and the passwords are not compromised but the briefcase contained a return acknowledgement report for accepted returns.	Risk is high. The information on the return acknowledgement report is easily accessible.

Deleting Taxpayer Information

Information may not be stored on partner owned or IRS loaned equipment once the filing season activities are completed. The information on all computers (both partner owned and IRS loaned), must be deleted (securely wiped) as part of the site closing activities. Deleting the information properly will prevent unauthorized disclosure of confidential information. IRS provided software encrypts all tax return data stored on the user's computer or on removable media.

Providers of electronic filing are reminded that they are required to retain a complete copy of the electronic portion of\ the tax return (which may be retained on magnetic media for desktop or the software vendor's website for online) until December 31 of the current tax year, which can be readily and accurately converted into an electronic transmission that the IRS can process.

Disposing of Taxpayer Information

Once taxpayer information is no longer required, it must be returned to the taxpayer or properly disposed of including burning or shredding the data.

Volunteer Safety

If a volunteer is threatened by a taxpayer at any time, first contact your local police department or 911 to have the taxpayer immediately removed from the facility. In addition, the incident should be reported 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

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. This information must be kept confidential and should not be disclosed 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 information provided through a FOIA request is used by the requester.

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. Refer to Publication 4961, *Volunteer Standards of Conduct – Ethics Training*, for complete details.

Form 13533, *Partner Sponsor Agreement*

Form 13533*, Partner Sponsor Agreement,* is requested annually. The Sponsor Agreement reiterates the key principles of privacy and confidentiality. By signing this agreement, the sponsor agrees to ensure their volunteers are aware of the standards of conduct, civil rights requirements, and privacy and confidentiality key principles. National and local SPEC offices must secure and maintain a signed Form 13533 for each partner. AARP and the military sponsor agreements are maintained at the SPEC Headquarters office. All other partner agreements are maintained in the territory office partner file.

Form 13533-A, *FSA Remote Sponsor Agreement*

Form 13533-A, *FSA Remote Sponsor Agreement*, is requested 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.

Statement of Assurance Concerning Civil Rights Compliance

By signing the *Sponsor Agreement*, Form 13533, 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 http://www.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 are obligated to comply with this assurance for one year from the date the Form 13533, *Sponsor Agreement*, is signed.

The organizational official whose signature appears on the *Partner Sponsor Agreement*, Form 13533, is authorized to sign this assurance and commit the "Partner" to the above provisions.

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 law suit 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 http://www.irs.gov/advocate for more information.

Reference Materials

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

- **Publication 1345 –** *Handbook for Authorized IRS e-file Providers*
- **Publication 1101 –** *Application Package and Guidelines for Managing a TCE Program*

- **Publication 1084 –** *Volunteer Site Coordinator's Handbook*
- **Publication 4600 –** *Safeguarding Taxpayer Information*
- **Publication 4557 –** *Safeguarding Taxpayer Data*
- **Publication 5027 (EN/SP)** – *Identity Theft Tool Kit*

Exhibit 1

Form **13533** (October 2015)	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 uphold the civil rights assurances as listed in the Pub 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**
(February 2014)

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.

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 refer any taxpayer questions about the FSA Program back to the third-party provider website for resolution.
- 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 where FSA link will be located _____

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.