Checklist for Safeguarding Taxpayer Data

ADMINISTRATIVE ACTIVITIES	ONGOING	DONE	N/A
Complete a Risk Assessment. Identify the risks and potential impacts of unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that can be used to access taxpayer data. How vulnerable is your customer's data to theft, disclosure, unauthorized alterations or unrecoverable loss? What can you do to reduce the impact to your customers and your business in such an event? What can you do to reduce vulnerability?	☐	☐	
Write and follow an Information Security Plan that:	☐	☐	
- Addresses every item identified in the risk assessment.	☐	☐	
- Defines safeguards you want affiliates and service providers to follow.	☐	☐	
- Requires a responsible person to review and approve the Information Security Plan.	☐	☐	
- Requires a responsible person to monitor, revise, and test the Information Security Plan on a periodic (recommended annual) basis to address any system or business changes or problems identified.	☐	☐	
Periodically (recommended annually) perform a Self-Assessment to:	☐	☐	
- Evaluate and test the security plan and other safeguards you have in place.	☐	☐	
- Document information safeguards deficiencies. Create and execute a plan to address them.	☐	☐	
Retain a copy of the Self-Assessment and ensure it is available for any potential reviews.	☐	☐	☐
If required by the FTC Privacy Rule, provide privacy notices and practices to your customers.	☐	☐	☐
Specify in contracts with service providers the safeguards they must follow and monitor how they handle taxpayer information.	☐	☐	☐
Ask service providers to give you a copy of their written security policy on safeguarding information.	☐	☐	☐

FACILITIES SECURITY	ONGOING	DONE	N/A
Protect from unauthorized access and potential danger (e.g., theft, floods and tornados) all places where taxpayer information is located.	☐	☐	
Write procedures that prevent unauthorized access and unauthorized processes.	☐	☐	
Assure that taxpayer information, including data on hardware and media, is not left un-secured on desks or photocopiers, in mailboxes, vehicles, trashcans or rooms in the office or at home where unauthorized access can occur.	☐	☐	
Authorize and control delivery and removal of all taxpayer information, including data on hardware and media.	☐	☐	
Lock doors to file rooms and/or computer rooms.	☐	☐	
Provide secure disposal of taxpayer information, such as shredders, burn boxes or temporary file areas until it can be securely disposed.	☐	☐	

PERSONNEL SECURITY	ONGOING	DONE	N/A
Create and distribute Rules of Behavior that describe responsibilities and expected behavior regarding computer information systems as well as paper records and usage of taxpayer data. Have all information system users' complete, sign, and submit an acknowledgement that they have read, understood, and agree to comply with the rules of behavior.	☐	☐	☐
An example of rules of behavior can be found in Appendix A of NIST SP-800 18 *Guide for Developing Security Plans for Federal Information Systems*.			
Ensure personnel from third-party providers such as service bureaus, contractors, and other businesses providing information technology services meet the same security requirements as those applied to your personnel.	☐	☐	☐
Address Rules of Behavior for computer system management.	☐	☐	☐
When interviewing prospective personnel, explain the expected Rules of Behavior.	☐	☐	☐
When possible, perform a background and/or reference check on new employees who will have contact with taxpayer information. Conduct background screenings that are appropriate to the sensitivity of an assigned position.	☐	☐	☐
Screen personnel prior to granting access to any paper or electronic data. This will help ensure their suitability for a position requiring confidentiality and trust.	☐	☐	☐
Have personnel who will have access to taxpayer information sign nondisclosure agreements on the use of confidential taxpayer information.	☐	☐	☐
Develop and enforce formal compliance policies and processes, including possible disciplinary action, for all personnel who do not comply with the businesses' established information security policies and procedures.	☐	☐	☐
Terminate access to taxpayer information (e.g., login IDs and passwords) for those employees who are terminated or who no longer need access.	☐	☐	☐
For each employee who is terminated, conduct an exit interview and ensure the employee returns property that allows access to taxpayer information (e.g., laptops, media, keys, identification cards and building passes).	☐	☐	☐
Train staff on Rules of Behavior for access, non-disclosure and safeguards of taxpayer information. Provide refresher training periodically.	☐	☐	☐

INFORMATION SYSTEMS SECURITY	ONGOING	DONE	N/A
Information systems include both automated and manual systems made up of people, machines and/or methods for collecting, processing, transmitting, storing, archiving and distributing data. To help ensure the accuracy, validity, consistency and reliability of taxpayer data, you should manage taxpayer data information systems based on the guidelines below.	☐	☐	
Grant access to taxpayer information systems only on a valid need-to-know basis that is determined by the individual's role within the business.	☐	☐	
Put in place a written contingency plan to perform critical processing in the event that your business is disrupted. It should include a plan to protect both electronic and paper taxpayer information systems. Identify individuals who will recover and restore the system after disruption or failure.	☐	☐	

Periodically test your contingency plan.	☐	☐	
Back up taxpayer data files regularly (e.g., daily or weekly) and store backup information at a secure location.	☐	☐	☐
Maintain hardware and software as needed and keep maintenance records.	☐	☐	☐

COMPUTER SYSTEMS SECURITY	**ONGOING**	**DONE**	**N/A**
Identify and authenticate computer system users who require access to electronic taxpayer information systems before granting them access.	☐	☐	☐
You can manage user identities by:			
- Identifying authorized users of electronic taxpayer information systems and grant specific access rights/privileges.	☐	☐	☐
- Assigning each user a unique identifier.	☐	☐	☐
- Verifying the identity of each user.	☐	☐	☐
- Disabling user identifiers after an organization-defined time period of inactivity.	☐	☐	☐
- Archiving user identities.	☐	☐	☐
Implement password management procedures that require strong passwords.	☐	☐	☐
Require periodic password changes.	☐	☐	☐
Disable and remove inactive user accounts.	☐	☐	☐
Protect electronic taxpayer information systems connected to the Internet with a barrier device (e.g., firewall, router or gateway). Any failure of these devices should not result in an unauthorized release of taxpayer data.	☐	☐	☐
When storing taxpayer information electronically, consider following best practices and store it on separate secure computers or media that are not connected to a network and that are password protected and encrypted.	☐	☐	☐
Encrypt taxpayer information when attached to email.	☐	☐	☐
Encrypt taxpayer information when transmitting across networks.	☐	☐	☐
Regularly update firewall, intrusion detection, anti-spyware, anti-adware, anti-virus software and security patches.	☐	☐	☐
Monitor computer systems for unauthorized access by reviewing system logs.	☐	☐	☐
Lock out computer system users after three consecutive invalid access attempts.	☐	☐	☐
Remove all taxpayer information once the retention period expires by using software designed to securely remove data from computers and media prior to disposing of hardware or media. The FTC Disposal Rule has information on how to dispose of sensitive data.	☐	☐	☐
As recommended by the FTC, reduce risks to computer systems by performing vulnerability scans and penetration tests periodically. You can learn more about this at the FTC Web site in their article “FTC Facts for Business – Security Check: Reducing Risks to Your Computer Systems.”	☐	☐	☐

MEDIA SECURITY	ONGOING	DONE	N/A
Store computer disks, removable media, tapes, compact disks, flash drives, audio and video recordings of conversations and meetings with taxpayers, and paper documents in a secure location, cabinet, or container.	☐	☐	
Secure media storage areas, including rooms, cabinets and computers by locks or key access. Where appropriate, employ an automated mechanism to ensure only authorized access.	☐	☐	
Restrict authorized access to media storage.	☐	☐	
Limit removal of taxpayer information to authorized persons and perform information access audits regularly.	☐	☐	
Securely remove all taxpayer information when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media that contain taxpayer information. The FTC Disposal Rule has information on how to dispose of sensitive data.	☐	☐	
Shred or burn paper documents before discarding them.	☐	☐	

CERTIFYING INFORMATION SYSTEMS FOR USE	ONGOING	DONE	N/A
Determine if risks are acceptable to certify systems for use.	☐	☐	☐
Sign an authority to operate.	☐	☐	
If you use a certified independent certification company, consider the following:	☐	☐	
- On a periodic (recommended annual) basis, have an independent individual or business with relevant security expertise, evaluate the security plans, controls, and any other safeguards implemented in your business against best practices.	☐	☐	
- Have a report generated from the audit that certifies that your business follows best practices.	☐	☐	
- Ensure the report highlights any deficiencies and provides recommendations for their correction.	☐	☐	
- Develop a plan for your business to correct any deficiencies found and to ensure that the plan is successfully executed.	☐	☐	
- Retain a copy of the audit report to ensure it is available for any potential reviews.	☐	☐	
- Be prepared to show how you mitigate risks.	☐	☐	