Guidance on Safeguarding Confidential Customer Information

This job aid provides guidance on how to safeguard confidential tax information at the local office.

General Rule

Confidential tax information may not be disclosed except as authorized by the Code of Virginia. This rule applies to all present and former local office employees.

Section 58.1-3, Code of Virginia, prescribes criminal penalties for divulging any information or business of any person, firm or corporation while in the performance of public duties. These criminal penalties apply to any agent, Clerk, Commissioner of the Revenue, Treasurer, or any State or local tax or revenue officer or employee, or any former officer or employee of any of these offices.

In addition to disclosure rules, The Taxpayer Browsing Protection Act makes unlawful the willful or negligent unauthorized inspection of federal tax information. “Browsing”, or unauthorized inspections, can carry a penalty for civil and criminal damages. The Department of Taxation (TAX) applies those same browsing protections to state tax information.

Under state and federal laws the following are confidential: any information acquired in the performance of your duties with respect to the transactions, income or business of any person, firm or corporation and any tax information provided to TAX by the customer, the customer’s representative or the IRS. Generally speaking, the information you receive regarding a customer’s affairs is protected from being released by provisions in the Code of Virginia.

Definitions

"Disclosure" is the making known of confidential tax information to any person in any manner. Disclosures are usually made either orally or in writing, but disclosures can also be made by action, as when you show someone a document that contains confidential tax information.

"What is confidential?" All the tax information regarding specific individuals and businesses is confidential. This is includes any tax information controlled, accumulated, gathered or stored by and in the offices of local Commissioners of the Revenue and Treasurers.

"Browsing" is willful or negligent unauthorized access or inspection of computerized or noncomputerized (hard copies) of customer records.

Examples of Browsing Violations
- Reviewing your family’s, friend’s or your own tax records without a work related reason
- Looking (and not telling) at customer information (electronic or paper) without a work related purpose

“Unauthorized Disclosure” is failure to secure customer and/or tax information to allow information accessible to the public or any employee who does not have a work related reason to view this information is an unauthorized disclosure. It is always the responsibility of the employee to exercise due diligence in safeguarding customer information, including tax returns and reports.

Examples of Unauthorized Disclosure

• Leaving customer information on your desk in an unsecured area or a TAX screen up and someone reads the information
• Revealing any tax information from any source, such as TAX systems, forms, returns or printouts, to a person you have not properly identified as the customer or as someone properly authorized by the customer to receive the information
• Discussing customer information in any public area, e.g. hallway, cafeteria, elevator and are overheard by others
• Discussing customer's information with coworkers who do not have a work related need to know the information
• For a child support case – releasing to a parent (custodial or non-custodial) if the other parent has filed a return
• For a lottery winner whose winnings are hit by a debt set-off because another person is using their SSN – divulging the name of the other person using that SSN
• For customers who file "married filing separate" – releasing information to a spouse not listed on the return
• Requests for information regarding whether another customer or business is registered for a given tax should be declined. You may not disclose whether another customer is registered for any particular type of tax.

Requirements to Safeguard State Information

Tax returns must be properly protected to insure confidentiality of the data. Whether you assist the customer to complete their return or accept the return to be forwarded to TAX for processing, tax returns must be protected at all times. When assisting customers with returns, ensure conversations can not be overheard or information compromised. Any working papers/documents that contain confidential information must be properly destroyed when no longer needed.

Only employees who work with state tax information are authorized to have access to the data. State tax information should only be used and stored in a controlled workspace. State tax information should be secured at the end of each work day. Questions or policies about storing and/or destroying tax information should be referred to TAX's Disclosure Officer.

State tax returns awaiting processing or mailing must be stored in a secure storage area such as a locking drawer, file cabinet or controlled area. Tax return and return documents must never be left unattended on desks or in areas with public access.

Office stationery, calendars, post-it notes, containing information such as customer names or account numbers should be properly secured depending on the type of information on them.

Regularly you must verify that your anti-virus software is up-to-date and functioning properly on all computers that contain or access state taxpayer records.

Destruction of Confidential Material

If confidential tax material must be destroyed then it must be done properly. The paper must be shredded to strips of 5/16 inch wide or smaller. It may be burned if care is taken to insure that all of the material was burned to such a state that it was unrecognizable. Other means producing similar results are also acceptable. Confidential material that can be read should never be thrown into any trash receptacle without proper destruction.

Disks and hard drives must be cleared or destroyed. Electronic storage media containing tax information must be electronically wiped clean or physically destroyed in such a manner that the information cannot be reconstructed.

Confidential material that is stored while waiting to be destroyed should be stored in a secured location to prevent unauthorized disclosure.