DOR Disclosure and Security Training for Safeguarding Information

As an employee of a state agency or a contractor ("Employee") who conducts business with the Massachusetts Department of Revenue ("DOR"), you may have access to confidential information regarding taxpayers and child support customers. This document summarizes your responsibilities in safeguarding DOR information.

Both state and federal laws protect the privacy and security of confidential information and create consequences for the failure to provide appropriate safeguards. Employees should only collect information that is necessary; access information only for business purposes; use information only for the purpose for which it is collected; keep information confidential; and disclose information only to those with statutory authority and a business need.

This guidance focuses on the following five key elements:

Identifying Confidential Information

All DOR information should be treated as confidential. Confidential information includes, but is not limited to:

- State and federal tax returns and return information
- Health insurance coverage information
- Wage reporting information
- Financial institution match information
- 14-day new hire information
- Child support information
- Information received from Commonwealth entities
- Information received from other states and entities
- "Personal Data" as defined in Mass General Law (MGL), Chapter 66A, that is maintained, created by, or submitted to the Department of Revenue
- "Personal Information" as defined in MGL Chapter 93H.

When you are uncertain whether the information is confidential, you should err on the side of caution and treat the information as confidential, and then ask your manager or supervisor for guidance.

Safeguarding Confidential Information

You are required to safeguard DOR information in your possession. The following are examples of best practices for safeguarding confidential information:

- Collect or access confidential information only for legitimate, work-related purposes.
- Use or disclose information only if authorized for a business need.
- Do not leave confidential information unattended.
- Do not leave or discuss confidential information in public areas.
- Share confidential information only if you have statutory authority and a business need.
- Discuss confidential matters only with authorized personnel.
- Retain confidential information only as long as necessary or as required by law.
- Dispose of confidential information securely (e.g., locked shred bin).
- Never access confidential information relating to you, family members, relatives, friends, neighbors, ex-spouses, or acquaintances for any purpose, including a business need.
- Follow a "clean desk practice." Clear your desk of any confidential information and lock your computer screen when leaving your workspace.
- Ensure fax numbers, email addresses or mailing names and addresses are correct.
- Confirm that the information being discussed pertains to the person to whom you are speaking.
- Beware of social engineering[1] schemes.

Unauthorized Access, Use and Disclosure

Unauthorized access, unauthorized use, or unauthorized disclosures may be intentional or unintentional.

Unauthorized access occurs when an individual receives or accesses confidential information that does not pertain to their work or assignments. Browsing information in applications or databases for a non-business purpose is prohibited.

Unauthorized use occurs when confidential information is used for a non-business purpose such as for personal use, financial gain, or harmful intent.

Unauthorized disclosure occurs when an entity or individual with authorization to receive confidential information discloses such information to another entity or individual who does not have the statutory authority and business need to obtain, view, or use the information.

Unintentional (unauthorized) disclosure is not deliberate and often the result of an error or lack of awareness such as:

- Notices intended for different taxpayers are comingled in the same envelope.
- Phone conversations about account information are held with the wrong taxpayer.
- Conversations involving confidential information are overheard.
- Faxes are retrieved by or delivered to the wrong employees.
- State property containing confidential information is lost or stolen.
- Information is mailed inadvertently to the wrong address.

[1] Social engineering is the act of stealing personal identification by deceiving people to make unwarranted disclosures.

Intentional (unauthorized) disclosure is knowingly giving confidential information in any manner to an individual, entity, or agency that is not authorized to obtain, view, or use the information. Examples include:

- Accessing and sharing details of a neighbor or friend's tax return with friends or family
- Accessing an ex- spouse's tax information.
- Accessing a child support case to help with a relative's child custody case.
- Telling your family or friends that you worked on a celebrity's tax return and providing the details.

Reporting Unauthorized Access, Use, and Disclosure

Immediately contact DOR's Administrative Affairs Division (AAD) at 617-626-2130 or RMABInformation@dor.state.ma.us and your supervisor to report an unauthorized access, use, or disclosure of confidential information or if you have any questions.

Although external agencies and parties might also require notification, you are only expected to report an unauthorized access, use or disclosure of confidential DOR Information to AAD, who will coordinate all required notifications. Early notification will enable AAD to assess the situation, recover data, coordinate notification of impacted taxpayers or child support customers, and contact the required federal and/or state agencies.

Understanding the Law

You must be vigilant in identifying confidential information. Both state and federal laws protect the privacy and security of information and impose consequences for the failure to do so.

As summarized in DOR's Compliance Agreement, browsing and unauthorized disclosure of information could result in fines, imprisonment, and/or disqualification from holding office in the Commonwealth. Additionally, browsing could lead to termination of employment with the Commonwealth or prevent you from working on a contract with the Commonwealth.

EMPLOYEE SIGNATURE

Name (print): _____

Signature: _____

Date: _____