



Get Started ►

2025 Non-Tax
Annual Access and
Disclosure Training

Introduction

As an employee or contractor, you may only access information for which you have been authorized and for which you have a *business need*. Although you may have a legitimate reason to access information, you have an obligation to protect what you have viewed, printed or stored.

Definition:

Access: The ability or privilege to make use of information.

You have a responsibility to maintain the confidentiality of personal, private and sensitive information entrusted to us. This information is referred to as “confidential information.”



Introduction

As an employee or contractor, you may only access information for which you have been authorized and for which you have a *business need*. Although you may have a legitimate reason to access information, you have an obligation to protect what you have viewed, printed or stored.

Definition:

Access: The ability or privilege to make use of information.

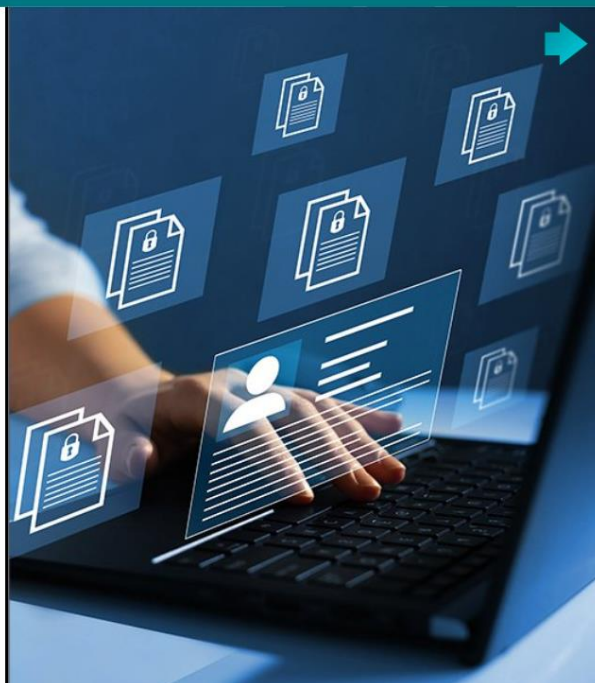
You have a responsibility to maintain the confidentiality of personal, private and sensitive information entrusted to us. This information is referred to as “confidential information.”

What is Confidential Information?

Confidential Information is information that can be directly or indirectly associated with a particular taxpayer, such as tax returns, return information, employee health insurance information, and driver's license information. It can exist in a variety of forms, such as e-mail, paper, electronic media, etc. It also includes any information that would compromise revenue.

Definition:

Tax Return and Return Information: Any tax or information return, declaration of estimated tax or claim for refund. This also includes any supporting schedules, attachments, or lists which are supplemental to, or part of, the return itself, whether they accompany the return or are provided at a later date.



What is Confidential Information?

Confidential Information is information that can be directly or indirectly associated with a particular taxpayer, such as tax returns, return information, employee health insurance information, and driver's license information. It can exist in a variety of forms, such as e-mail, paper, electronic media, etc. It also includes any information that would compromise revenue.

Definition:

Tax Return and Return Information: Any tax or information return, declaration of estimated tax or claim for refund. This also includes any supporting schedules, attachments, or lists which are supplemental to, or part of, the return itself, whether they accompany the return or are provided at a later date.

What is Confidential Information?

Such information also includes: Audit Division selection criteria; dollar tolerance procedures; audit work papers and documents; information submitted to or developed by the Department in connection with bonding and licensing requirements; mainframe, personal computer, laptop, electronic mail and other passwords and access procedures; computer programs and design documentation; ongoing, inactive or closed investigative reports and associated work papers; audit reports including those issued by the Bureau of Internal Audit and Quality Control, Office of the State Comptroller, Division of Budget and others; tax compliance records and documents obtained in connection with collection activities; and litigation, prosecution, or enforcement documentation.



What is Confidential Information?

Such information also includes: Audit Division selection criteria; dollar tolerance procedures; audit work papers and documents; information submitted to or developed by the Department in connection with bonding and licensing requirements; mainframe, personal computer, laptop, electronic mail and other passwords and access procedures; computer programs and design documentation; ongoing, inactive or closed investigative reports and associated work papers; audit reports including those issued by the Bureau of Internal Audit and Quality Control, Office of the State Comptroller, Division of Budget and others; tax compliance records and documents obtained in connection with collection activities; and litigation, prosecution, or enforcement documentation.

Introduction

Examples of confidential information:

- Social Security Number (SSN)
- Taxpayer return information
- Wages
- Taxpayer filing history
- Information related to any current or potential audit/investigation activity
- Official personnel information
- Audit work papers or anything else that contains information taken from tax returns or schedules
- Computer programs and information system design documentation



Introduction

Examples of confidential information:

- Social Security Number (SSN)
- Taxpayer return information
- Wages
- Taxpayer filing history
- Information related to any current or potential audit/investigation activity
- Official personnel information
- Audit work papers or anything else that contains information taken from tax returns or schedules
- Computer programs and information system design documentation



Introduction



Need to Know

Accessing confidential information must be limited to what you “need to know” in order to perform your official responsibilities. **Official duties NEVER include** accessing your own tax records or those of co-workers, neighbors, friends or family. You are **NOT** allowed to access your own tax records or those of co-workers, neighbors, friends or family for training, testing, or other work-related programming activities.

Without the “need to know,” you are not authorized to access, attempt to access, request or modify confidential information.

Introduction

Need to Know

Accessing confidential information must be limited to what you “need to know” in order to perform your official responsibilities. **Official duties NEVER include** accessing your own tax records or those of co-workers, neighbors, friends or family. You are **NOT** allowed to access your own tax records or those of co-workers, neighbors, friends or family for training, testing, or other work-related programming activities.

Without the “need to know,” you are not authorized to access, attempt to access, request or modify confidential information.

Introduction

Confidential information **CANNOT** be disclosed or shared with others unless they are properly authorized and have a “need to know.” By completing this training you are not only acknowledging your understanding of these concepts, you are also declaring your personal commitment to maintaining the confidentiality and privacy of taxpayer information.

Definition:

Disclosure: Making information known in any manner, including phone calls, faxes, letters, discussions or any electronic means, such as e-mail. This includes disclosures to yourself of information you are not entitled to know.



Introduction

Confidential information **CANNOT** be disclosed or shared with others unless they are properly authorized and have a “need to know.” By completing this training you are not only acknowledging your understanding of these concepts, you are also declaring your personal commitment to maintaining the confidentiality and privacy of taxpayer information.

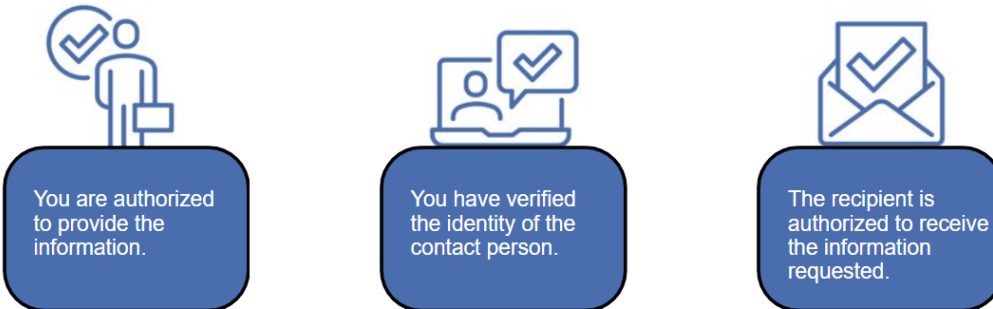
Definition:

Disclosure: Making information known in any manner, including phone calls, faxes, letters, discussions or any electronic means, such as e-mail. This includes disclosures to yourself of information you are not entitled to know.

Introduction



DO NOT disclose confidential or sensitive information, including tax information unless:



DO NOT disclose any information if you are unsure whether someone is authorized to receive that information.

Introduction

DO NOT disclose confidential or sensitive information, including tax information unless:

- You are authorized to provide the information.
- You have verified the identity of the contact person.
- The recipient is authorized to receive the information requested.

DO NOT disclose any information if you are unsure whether someone is authorized to receive that information.

KNOWLEDGE CHECK

1. Information system design documentation is confidential
 - ☒ A. True
 - ☐ B. False
2. It is okay to access your own tax records for testing purposes.
 - ☒ A. True
 - ☐ B. False
3. One of my co-workers asked me to look up someone's information and I was not informed why. It is OK to do this.
 - ☒ A. True
 - ☐ B. False

You have completed this Knowledge Check page

[Continue ►](#)

KNOWLEDGE CHECK

1. Information system design documentation is confidential

- A. True
- B. False

That's not the correct answer. Information system design documentation IS confidential.

2. It is okay to access your own tax records for testing purposes.

- A. True

That's not the correct answer. It is NEVER ok to access one's own tax records.

- B. False

3. One of my co-workers asked me to look up someone's information and I was not informed why. It is OK to do this.

- A. True

That's not the correct answer. Information should only be accessed on a "Need to Know" basis. It is a coworker asking without a reason and not a supervisor who articulates business reason for making the access.

- B. False

 **Department of
Taxation and Finance**

HELP COURSE MAP EXIT 9
of 54

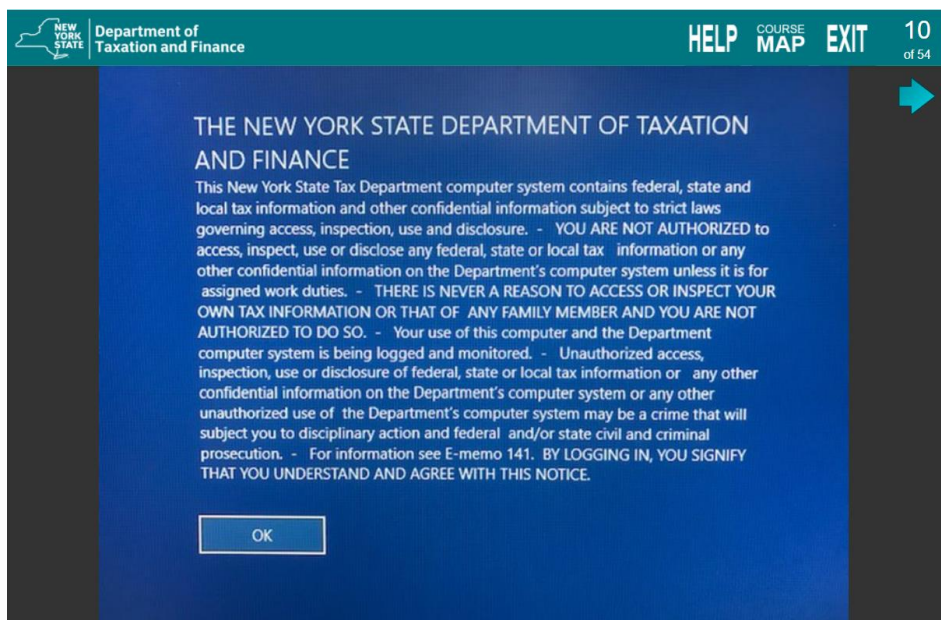
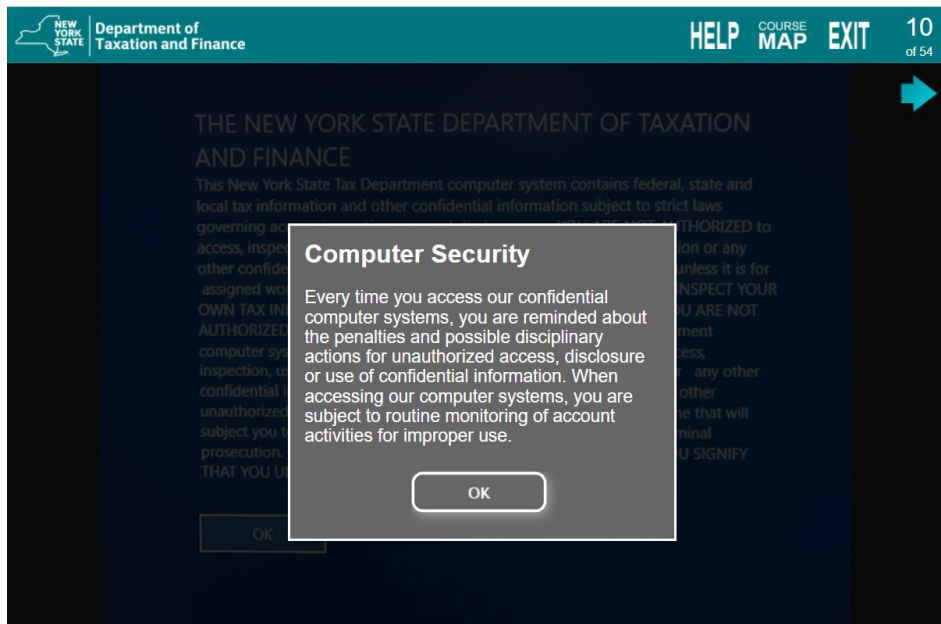
Public Officers Law

[Section 73](#) and [Section 74](#) of the Public Officers Law provides standards of conduct and ethics of all state officers, employees and party officers.



Public Officers Law

[Section 73](#) and [Section 74](#) of the Public Officers Law provides standards of conduct and ethics of all state officers, employees and party officers.



Computer Security

Every time you access our confidential computer systems, you are reminded about the penalties and possible disciplinary actions for unauthorized access, disclosure or use of confidential information. When accessing our computer systems, you are subject to routine monitoring of account activities for improper use.

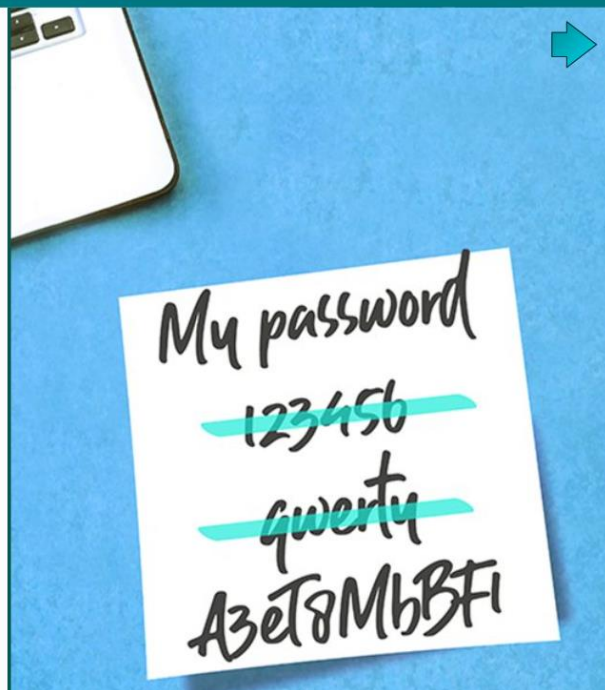
Computer Security

Password Rules:

Each person is responsible for any activity that takes place under his/her USER ID. Following the PASSWORD guidelines below, will help secure all activity performed under your USER ID.

Password Guidelines:

- Use PASSWORDS that CANNOT be easily guessed.
- Never let anyone use your USER ID or PASSWORD to log in.
- Never share your PASSWORD with anyone, not even your supervisor or Help Desk Staff.
- Do NOT save your PASSWORD (on paper or electronically) in a place that may be accessible by another individual.
- Do NOT use the same PASSWORD for different systems (e.g. home PC, personal e-mail account, personal bank account, etc...)



Computer Security

Password Rules:

Each person is responsible for any activity that takes place under his/her USER ID. Following the PASSWORD guidelines below, will help secure all activity performed under your USER ID.

Password Guidelines:

- Use PASSWORDS that CANNOT be easily guessed.
- Never let anyone use your USER ID or PASSWORD to log in.
- Never share your PASSWORD with anyone, not even your supervisor or Help Desk Staff.
- Do NOT save your PASSWORD (on paper or electronically) in a place that may be accessible by another individual.
- Do NOT use the same PASSWORD for different systems (e.g. home PC, personal e-mail account, personal bank account, etc...)

NEW YORK STATE Department of Taxation and Finance

HELP COURSE MAP EXIT 12 of 54

Computer Security

Password Retention Pop-up

You may see one of the following messages below when a password is required to perform job functions such as accessing NY.GOV:

- **DO NOT** click "Yes" or "Save Password"
- **DO CLICK** "No," "Not for this site," or "Never for This Website"

Password: [Masked Password Field]

Would you like to store your password for ny.gov?
Why am I seeing this? Yes Not for this site

Would you like to save this password in your iCloud Keychain for AutoFill on all your devices?
You can view and remove saved passwords in Safari settings.
Save Password
Never for This Website
Not Now

Computer Security

Password Retention Pop-up

You may see one of the following messages below when a password is required to perform job functions such as accessing NY.GOV:

- **DO NOT** click "Yes" or "Save Password"
- **DO CLICK** "No," "Not for this site," or "Never for This Website"

Department of
Taxation and Finance

HELPCOURSE
MAPEXIT

13
of 54



Computer Security

Security Guidelines for Tax Computer Use:

Always log off, lock up (Ctrl, Alt & Delete) or shut down your computer whenever you are away from it.

Locking your computer can be done by pressing Ctrl, Alt & Delete, then click on *Lock this computer* or simply click the Windows Key & L. If using a virtual machine, press Ctrl, Alt & Insert, then click on "Lock this computer."

Be aware of others around you when looking at confidential information.

Report any inappropriate activity directly to the Office of Internal Affairs (518) 451-1566.

DO NOT install unapproved files or software on your computer.

Computer Security

Security Guidelines for Tax Computer Use:

Always log off, lock up (Ctrl, Alt & Delete) or shut down your computer whenever you are away from it.

Locking your computer can be done by pressing Ctrl, Alt & Delete, then click on *Lock this computer* or simply click the Windows Key & L. If using a virtual machine, press Ctrl, Alt & Insert, then click on "Lock this computer."

Be aware of others around you when looking at confidential information.

Report any inappropriate activity directly to the Office of Internal Affairs (518) 451-1566.

DO NOT install unapproved files or software on your computer.



KNOWLEDGE CHECK



1. The Help desk calls indicating that your password does not meet current complexity requirements. The person on the phone asks you to create a new password and provide the new password verbally over the phone.

It is okay to refuse to provide your password and end the phone call with the Help Desk.

- ☒ A. True
☐ B. False



2. When you need to leave the general area of your computer for only a few minutes, it's okay to leave it unlocked as long as no taxpayer information is displayed and your desktop screen is showing on your monitor.

- ☐ A. True
☒ B. False

You have completed this
Knowledge Check page

[Continue ►](#)

KNOWLEDGE CHECK

1. The Help desk calls indicating that your password does not meet current complexity requirements. The person on the phone asks you to create a new password and provide the new password verbally over the phone.

It is okay to refuse to provide your password and end the phone call with the Help Desk.

- A. True
B. False

That's not the correct answer. Never give your password to anyone. Helpdesk staff will NEVER ask for your password.

2. When you need to leave the general area of your computer for only a few minutes, it's okay to leave it unlocked as long as no taxpayer information is displayed and your desktop screen is showing on your monitor.

- A. True

You answered the question incorrectly. To prevent a breach of computer security, you should ALWAYS lock (Ctrl, Alt & Delete) your computer when unattended.

- B. False

KNOWLEDGE CHECK



3. I logged into my NY.GOV account for work and a pop-up appeared asking if I want the system to remember my password. It is OK for me to click "Yes."

- ☒ A. True
- ☐ B. False

You have completed this
Knowledge Check page

[Continue ►](#)

KNOWLEDGE CHECK

3. I logged into my NY.GOV account for work and a pop-up appeared asking if I want the system to remember my password. It is OK for me to click "Yes."

A. True

That's not the correct answer. You must click "no," "not for this site," or "never for this website" when a pop-up appears asking you to store your password.

B. False



Information Protection

The New York State Information Security Breach and Notification Act requires New York State entities to contact affected persons, without unreasonable delay, after any breach of security, unauthorized access or unauthorized release of computerized private data.

Additionally, the Department has enhanced its reporting requirements to also include hard-copy confidential documents.



Information Protection

The New York State Information Security Breach and Notification Act requires New York State entities to contact affected persons, without unreasonable delay, after any breach of security, unauthorized access or unauthorized release of computerized private data.

Additionally, the Department has enhanced its reporting requirements to also include hard-copy confidential documents.



Information Protection

All Department employees are to report any work-related incident that they believe constitutes an *information security breach* or *unauthorized disclosure* of confidential tax information or private information.

Private information is information that uniquely identifies an individual such as a person's name along with a Social Security Number or driver's license ID or financial information that would permit access to an individual's financial account.



Information Protection

All Department employees are to report any work-related incident that they believe constitutes an *information security breach* or *unauthorized disclosure* of confidential tax information or private information.

Private information is information that uniquely identifies an individual such as a person's name along with a Social Security Number or driver's license ID or financial information that would permit access to an individual's financial account.

Information Protection



Definition:

Information Security Breach: An incident in which sensitive, protected or confidential information has potentially been viewed, stolen or used (intentionally or unintentionally) by an individual unauthorized to do so.



Information Protection

Definition:

Information Security Breach: An incident in which sensitive, protected or confidential information has potentially been viewed, stolen or used (intentionally or unintentionally) by an individual unauthorized to do so.

Information Protection



Definition:

Inadvertent Unauthorized Disclosure: Unintentionally making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information. This could also include unauthorized disclosure or inadvertent unauthorized disclosure.



Information Protection

Definition:

Inadvertent Unauthorized Disclosure: Unintentionally making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information. This could also include unauthorized disclosure or inadvertent unauthorized disclosure.

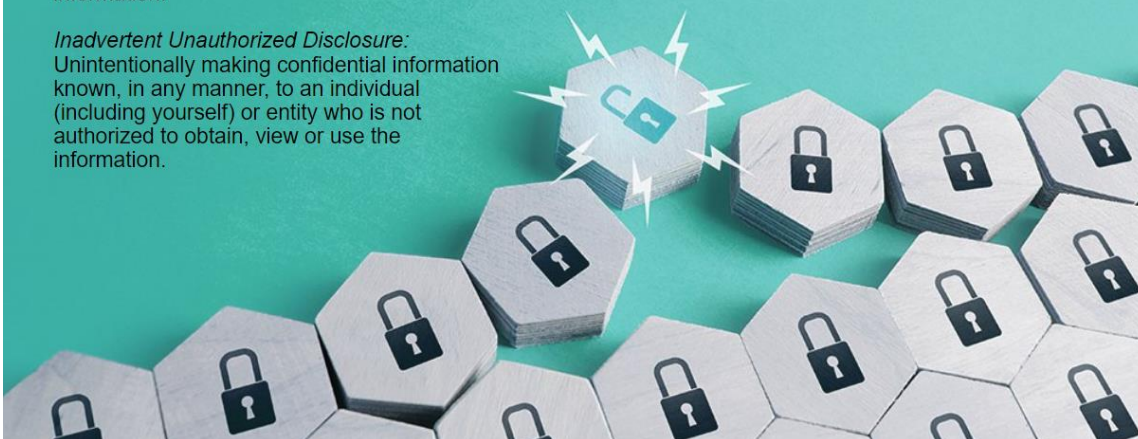
Information Protection



Definition:

Unauthorized Disclosure: Making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information.

Inadvertent Unauthorized Disclosure: Unintentionally making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information.



Information Protection

Definition:

Unauthorized Disclosure: Making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information.

Inadvertent Unauthorized Disclosure: Unintentionally making confidential information known, in any manner, to an individual (including yourself) or entity who is not authorized to obtain, view or use the information.



Department of
Taxation and Finance

HELP

COURSE
MAP

EXIT

21
of 54

Information Protection

Examples of an Unauthorized Disclosure would include:

Inadvertent Unauthorized Disclosure

Some examples are:

- Mail or faxes sent to the wrong party.
- A briefcase containing taxpayer information was left unsupervised and its location cannot be determined.
- Documents containing Federal Tax Information (FTI) cannot be located.

Unauthorized Disclosure

Some examples are:

- An employee accesses his daughter's tax return and shares it with her.
- An employee shares with friends the tolerance amounts that Audit has established for issuing bills.

All of the above would be considered an Information Security Breach.



Information Protection

Examples of an Unauthorized Disclosure would include:

Inadvertent Unauthorized Disclosure

Some examples are:

- Mail or faxes sent to the wrong party.
- A briefcase containing taxpayer information was left unsupervised and its location cannot be determined.
- Documents containing Federal Tax Information (FTI) cannot be located.

Unauthorized Disclosure

Some examples are:

- An employee accesses his daughter's tax return and shares it with her.
- An employee shares with friends the tolerance amounts that Audit has established for issuing bills.

All of the above would be considered an Information Security Breach.

Information Protection

Reporting Requirements

ITS staff and ITS contractors:

- Immediately report any suspected inappropriate activity, unauthorized access, unauthorized disclosure, or any other suspected breaches to your appropriate manager and the Information Security Officer (ISO)/designated security representative.
- Follow the reporting procedures found on the NYS ITS EISO incident link – <http://its.ny.gov/incident-reporting>.

Everyone else:

To report an unintentional information security breach, immediately contact the DTF Information Security Office.

To report any inappropriate activity (such as unauthorized access or disclosure), immediately contact the DTF Office of Internal Affairs (518) 451-1566.



Information Protection

Reporting Requirements

ITS staff and ITS contractors:

- Immediately report any suspected inappropriate activity, unauthorized access, unauthorized disclosure, or any other suspected breaches to your appropriate manager and the Information Security Officer (ISO)/designated security representative.
- Follow the reporting procedures found on the NYS ITS EISO incident link – <http://its.ny.gov/incident-reporting>.

Everyone else:

To report an unintentional information security breach, immediately contact the DTF Information Security Office.

To report any inappropriate activity (such as unauthorized access or disclosure), immediately contact the DTF Office of Internal Affairs (518) 451-1566.

HELP

COURSE MAP

EXIT

23 of 54

"Access Denied" error message and email

The Department prevents persons with access to e-MPIRE from accessing certain records which are flagged as being associated with the user and therefore are inaccessible. There are a variety of reasons for an account to be flagged, for example, a spouse listed on a primary return for the employee who now files returns independently.

When an employee goes to e-MPIRE and enters information to look at one of these accounts, they will receive a message and email that looks like this.

This message may also be generated from work that is randomly pushed to an employee through automated workflow processes. If you receive this message you must immediately notify your supervisor to document the reason you were attempting to access that account. The Office of Internal Affairs will automatically receive notification of the employee's attempted access.

The screenshot shows the e-MPIRE interface with the title 'Individual Taxpayer Profile Inquiry'. It includes tabs for Client Information, Account Information, Work Management, and Special Services. Below these are fields for ID, Name, Address, Associated ID, and Associated Name. A search bar is visible with a dropdown menu set to '9 Character ID' and the value '123456789'. A red error message at the bottom reads: 'S06527 ACCESS DENIED: See Executive Memorandum E-141. Contact your supervisor now'.

"Access Denied" error message and email

The Department prevents persons with access to e-MPIRE from accessing certain records which are flagged as being associated with the user and therefore are inaccessible. There are a variety of reasons for an account to be flagged, for example, a spouse listed on a primary return for the employee who now files returns independently.

When an employee goes to e-MPIRE and enters information to look at one of these accounts, they will receive a message and email that looks like this.

This message may also be generated from work that is randomly pushed to an employee through automated workflow processes. If you receive this message you must immediately notify your supervisor to document the reason you were attempting to access that account. The Office of Internal Affairs will automatically receive notification of the employee's attempted access.

Telecommuting policies

To protect taxpayer information in a remote work setting, some important things to consider:

- Treat the home workspace as if it is a physical office location.
- Do not leave your computer, laptop, or other work devices unlocked while unattended.
- Do not allow family members (or other unauthorized people) to use your work devices.
- Turn off voice enabled "listening" technology devices such as Amazon Alexa, Google Home, Siri, interconnected toys (Cloud Pet, Smart Toy, Hello Barbie, etc), or other technologies that may record and transmit photos, videos, or voice on personal devices while working in the same room.
- Do not write down sensitive taxpayer information at home and leave it unattended.

(Continued on next slide)



Telecommuting policies

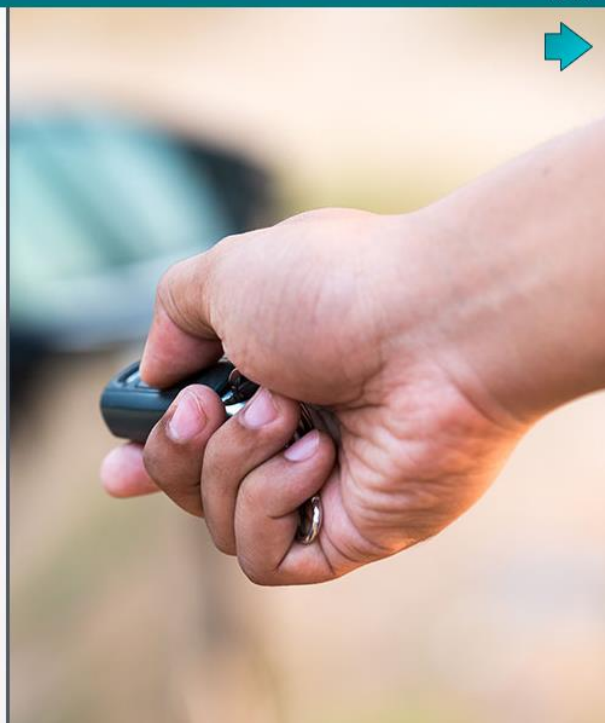
To protect taxpayer information in a remote work setting, some important things to consider:

- Treat the home workspace as if it is a physical office location.
- Do not leave your computer, laptop, or other work devices unlocked while unattended.
- Do not allow family members (or other unauthorized people) to use your work devices.
- Turn off voice enabled "listening" technology devices such as Amazon Alexa, Google Home, Siri, interconnected toys (Cloud Pet, Smart Toy, Hello Barbie, etc), or other technologies that may record and transmit photos, videos, or voice on personal devices while working in the same room.
- Do not write down sensitive taxpayer information at home and leave it unattended.

Telecommuting policies

To protect taxpayer information in a remote work setting, some important things to consider:

- If you MUST leave work devices in the car, the car must be locked, and devices must not be visible.
- If you have written down or printed [confidential taxpayer information](#), securely bring it back to the office for secure destruction.



Telecommuting policies

To protect taxpayer information in a remote work setting, some important things to consider:

- If you MUST leave work devices in the car, the car must be locked, and devices must not be visible.
- If you have written down or printed [confidential taxpayer information](#), securely bring it back to the office for secure destruction.



KNOWLEDGE CHECK

1. You're working from home and your partner enters your workspace to say hello. They want to see what you are doing for work and help you use your computer. What should you do?
 - ☐ A. Let them sit with you and see what you are doing, no one will know since you are at home.
 - ☐ B. Let them sit with you and make sure your important confidential work is closed before showing them what you are doing.
 - ☐ C. Lock your computer and tell them that your work is confidential and cannot be shared.

Knowledge Check

1. You're working from home and your partner enters your workspace to say hello. They want to see what you are doing for work and help you use your computer. What should you do?

A. Let them sit with you and see what you are doing, no one will know since you are at home.

B. Let them sit with you and make sure your important confidential work is closed before showing them what you are doing.

That's not the correct answer. You should lock your computer when you need to attend to any family matters while telecommuting. While you may not have confidential information displayed, your work should never be visible or seen by someone without a need to know (regardless of who they are), and your work devices should never be used by anyone without authority to use them.

C. Lock your computer and tell them that your work is confidential and cannot be shared

Internal Revenue Service

Internal Revenue Service (IRS) Information:

Internal Revenue Code Sections 6103(d), 7213 (a)(2), 7213A and 7431:

- Allow disclosure of federal tax information to state tax agencies for tax administration.
- Impose penalties and civil damages for unauthorized inspection and disclosure.

Confidential information received from the IRS is referred to as *Federal Tax Information (FTI)*. All FTI received from the IRS is subject to federal requirements and cannot be re-disclosed, even with other agencies, without prior written permission from the IRS.



Internal Revenue Service

Internal Revenue Service (IRS) Information:

Internal Revenue Code Sections 6103(d), 7213 (a)(2), 7213A and 7431:

- Allow disclosure of federal tax information to state tax agencies for tax administration.
- Impose penalties and civil damages for unauthorized inspection and disclosure.

Confidential information received from the IRS is referred to as *Federal Tax Information (FTI)*. All FTI received from the IRS is subject to federal requirements and cannot be re-disclosed, even with other agencies, without prior written permission from the IRS.

Some examples of FTI are:

- Federal returns received from the IRS
- Print screens of FTI on e-MPIRE
- Information written down from viewed FTI
- Federal transcripts from Transcript Delivery System (TDS)

Definition:

Federal Tax Information (FTI): FTI is any return or return information (paper, CDs, electronic files, etc.) received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI information includes any information created by the recipient that is derived from return or return information. **For example, an updated address based on information obtained from the IRS is considered to be FTI.**



Some examples of FTI are:

- Federal returns received from the IRS
- Print screens of FTI on e-MPIRE
- Information written down from viewed FTI
- Federal transcripts from Transcript Delivery System (TDS)

Definition:

Federal Tax Information (FTI): FTI is any return or return information (paper, CDs, electronic files, etc.) received from the IRS or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI information includes any information created by the recipient that is derived from return or return information. **For example, an updated address based on information obtained from the IRS is considered to be FTI.**

Internal Revenue Service

(IRS) Information, continued...

The IRS requires that FTI be tracked from the time it is received to the time it is destroyed.

- Whenever employees are away from their desks, all FTI must be secured. An example of a secured location is a locked filing cabinet or locked desk drawer.
- Federal tax information sent to another location must be double-sealed (one envelope inside another envelope).



Internal Revenue Service

(IRS) Information, continued...

The IRS requires that FTI be tracked from the time it is received to the time it is destroyed.

- Whenever employees are away from their desks, all FTI must be secured. An example of a secured location is a locked filing cabinet or locked desk drawer.
- Federal tax information sent to another location must be double-sealed (one envelope inside another envelope).

Information Protection

Properly Dispose of Confidential Information (FTI):

- To properly destroy papers containing confidential information or FTI you must place them in a locked confidential destruction bin.
- If you see an unlocked bin, please notify your supervisor.
- Do NOT place any papers containing confidential information / FTI in the trash or in recycling (3R's) baskets.
- Do NOT use shredders – the models we have are not IRS compliant.
- You must properly dispose of all electronic portable media, such as diskettes, CDs, DVDs, flash drives, computer tapes, optical disks, hard drives, removable drives of any kind, or any other USB connected storage media that contains confidential information.

*Please refer to the [Disposal of Electronic Media Policies and Procedures](#) to view the policies and procedures for the secure handling and disposal of confidential information.



Information Protection

Properly Dispose of Confidential Information (FTI):

- To properly destroy papers containing confidential information or FTI you must place them in a locked confidential destruction bin.
- If you see an unlocked bin, please notify your supervisor.
- Do NOT place any papers containing confidential information / FTI in the trash or in recycling (3R's) baskets.
- Do NOT use shredders – the models we have are not IRS compliant.
- You must properly dispose of all electronic portable media, such as diskettes, CDs, DVDs, flash drives, computer tapes, optical disks, hard drives, removable drives of any kind, or any other USB connected storage media that contains confidential information.

*Please refer to the [Disposal of Electronic Media Policies and Procedures](#) to view the policies and procedures for the secure handling and disposal of confidential information.



Internal Revenue Service

FTI Logs:

IRS requires that a tracking system is established to identify and track the location of electronic and non-electronic FTI where it is used from the time it is received to the date it is disposed of.

For examples of suggested tracking elements, see [IRS Publication 1075](#): Section 3.2, pages 13 & 14.



Internal Revenue Service

FTI Logs:

IRS requires that a tracking system is established to identify and track the location of electronic and non-electronic FTI where it is used from the time it is received to the date it is disposed of.

For examples of suggested tracking elements, see [IRS Publication 1075](#): Section 3.2, pages 13 & 14.

IRS information, continued...



Important Reminder:

When IRS information is commingled with DTF files, either paper or electronic, the entire file is considered to be FTI and must be labeled and safeguarded in accordance with IRS requirements. The Inspection or Disclosure Limitation Labels used to identify all FTI may be requested by emailing the Office of Disclosure and Government Exchange at tax.sm.Disclosure.

Inspection or Disclosure Limitations

Unauthorized inspection or disclosure, printing, or publishing of any Federal return or return information, or any information therefrom, may be punishable by fine or imprisonment and in the case of Federal officers or employees, dismissal from office or employment. See section 7213 and 7213A of the Internal Revenue Code and 18 U.S.C. section 1905. In addition, code section 7431 provides for civil damages for unauthorized inspection or disclosure of such information. Tapes should be degaussed after they have served their purpose, disposed of in accordance with Publication 1075 disposition guidelines or returned to the IRS.

Department of the Treasury
Internal Revenue Service

Notice 129A (Rev.12-97)
Cat No. 45547W

Definition: Commingling: When Department information is combined with federal tax information, either paper or electronic, it is considered to be commingled and is to be treated as FTI.

Federal tax return and/or return information received directly from a taxpayer or third party is **NOT** considered FTI.

Electronic files must use a naming convention that clearly identifies the file as containing FTI for example: FED.filename or FTI.filename.

IRS information, continued...

Important Reminder:

When IRS information is commingled with DTF files, either paper or electronic, the entire file is considered to be FTI and must be labeled and safeguarded in accordance with IRS requirements. The Inspection or Disclosure Limitation Labels used to identify all FTI may be requested by emailing the Office of Disclosure and Government Exchange at tax.sm.Disclosure.

Inspection or Disclosure Limitations

Unauthorized inspection or disclosure, printing, or publishing of any Federal return or return information, or any information therefrom, may be punishable by fine or imprisonment and in the case of Federal officers or employees, dismissal from office or employment. See section 7213 and 7213A of the Internal Revenue Code and 18 U.S.C. section 1905. In addition, code section 7431 provides for civil damages for unauthorized inspection or disclosure of such information. Tapes should be degaussed after they have served their purpose, disposed of in accordance with Publication 1075 disposition guidelines or returned to the IRS.

Department of the Treasury
Internal Revenue Service

Notice 129A (Rev.12-97)
Cat No. 45547W

Definition: Commingling: When Department information is combined with federal tax information, either paper or electronic, it is considered to be commingled and is to be treated as FTI.

Federal tax return and/or return information received directly from a taxpayer or third party is **NOT** considered FTI.

Electronic files must use a naming convention that clearly identifies the file as containing FTI for example: FED.filename or FTI.filename.



KNOWLEDGE CHECK



1. What is the federal penalty for unauthorized disclosure of FTI?

- ☐ A. Up to 5 years in prison.
- ☐ B. Fine up to \$5,000.
- ☐ C. None of the above.
- ☐ D. Both A and B.

You have completed this
Knowledge Check page

[Continue](#) ►

KNOWLEDGE CHECK

1. What is the federal penalty for unauthorized disclosure of FTI?

- A. Up to 5 years in Prison
- B. Fine up to \$5,000.
- C. None of the above.

That's not the correct answer.

- D. Both A and B.



Social Security

Social Security Administration (SSA) Information:

DTF receives SSA data which is considered confidential federal information. The Death Match File is one of the files DTF receives from SSA.

Penalty provisions under U.S. Department of Commerce, National Technical Information Services (NTIS) Section 203 of the Bipartisan Budget Act of 2013, 15 CFR 1110.200 imposes a penalty of \$1,000 for each of the below infractions:

- Unauthorized disclosure of the Death Match File Information.
- Use of any deceased individual's Death Match File information for any purpose other than a legitimate fraud prevention interest or a legitimate business pursuant to a law, governmental rule, regulation or fiduciary duty.


Social Security

Social Security Administration (SSA) Information:

DTF receives SSA data which is considered confidential federal information. The Death Match File is one of the files DTF receives from SSA.


Penalty provisions under U.S. Department of Commerce, National Technical Information Services (NTIS) Section 203 of the Bipartisan Budget Act of 2013, 15 CFR 1110.200 imposes a penalty of \$1,000 for each of the below infractions:

- Unauthorized disclosure of the Death Match File Information.
- Use of any deceased individual's Death Match File information for any purpose other than a legitimate fraud prevention interest or a legitimate business pursuant to a law, governmental rule, regulation, or fiduciary duty.


Department of
Taxation and Finance

HELPCOURSE
MAPEXIT

35
of 54



Law



Important Information:

You should be aware of several laws and legislative acts that address penalties if improper disclosure of confidential information occurs:


- Privacy Act of 1974
- New York State Tax Law
- New York State Penal Law
- Internal Revenue Code

Law

Important Information:

You should be aware of several laws and legislative acts that address penalties if improper disclosure of confidential information occurs:

- Privacy Act of 1974
- New York State Tax Law
- New York State Penal Law
- Internal Revenue Code



Department of
Taxation and Finance

HELP

COURSE
MAP

EXIT

36
of 54



Law


Privacy Act of 1974, 5 U.S.C. 552a:

Under Section 5 U.S.C 552a(i)(1) of the Privacy Act of 1974, it is unlawful for you to willfully disclose confidential information in any manner to any person not entitled to receive it. In doing so you would be guilty of a misdemeanor and fined up to \$5,000.

Law

Privacy Act of 1974, 5 U.S.C. 552a:

Under Section 5 U.S.C 552a(i)(1) of the Privacy Act of 1974, it is unlawful for you to willfully disclose confidential information in any manner to any person not entitled to receive it. In doing so you would be guilty of a misdemeanor and fined up to \$5,000.



Department of
Taxation and Finance

HELP COURSE MAP EXIT 37
of 54

Law


New York State Penalties:

Under New York State Tax Law Section 1825, it is a crime for you to make an unauthorized disclosure of confidential New York State Tax information.

New York State Penal Law Section 156 imposes additional charges for unauthorized access, computer trespass or computer tampering, which can be misdemeanors or felonies.

Punitive Actions For Violating NYS Tax Law:

- Possible dismissal from employment.
- Possible criminal prosecution.
- A fine up to \$10,000, up to one year in jail, or both.
- Possible prohibition from holding state service for five years.



Law

New York State Penalties:

Under New York State Tax Law Section 1825, it is a crime for you to make an unauthorized disclosure of confidential New York State Tax information.

New York State Penal Law Section 156 imposes additional charges for unauthorized access, computer trespass or computer tampering, which can be misdemeanors or felonies.

Punitive Actions For Violating NYS Tax Law:

- Possible dismissal from employment.
- Possible criminal prosecution.
- A fine up to \$10,000, up to one year in jail, or both.
- Possible prohibition from holding state service for five years.



Department of
Taxation and Finance

HELP COURSE MAP EXIT 38
of 54

Law

Federal Penalties:

Under Section 7213 of the Internal Revenue Code, it is a felony to make an unauthorized disclosure of federal tax information.

Penalties Include:

- A fine up to \$5,000, up to 5 years in prison, or both.
- Cost of prosecution.
- Possible disciplinary action.



Law

Federal Penalties:

Under Section 7213 of the Internal Revenue Code, it is a felony to make an unauthorized disclosure of federal tax information.

Penalties Include:

- A fine up to \$5,000, up to 5 years in prison, or both.
- Cost of prosecution.
- Possible disciplinary action.

Law

Federal Penalties, continued...

Under Section 7213A of the Internal Revenue Code, it is a crime to browse federal tax data without a business need.

Penalties Include:

- A fine not exceeding \$1,000, imprisonment of not more than one year, or both.
- Cost of prosecution.



Law

Federal Penalties, continued...

Under Section 7213A of the Internal Revenue Code, it is a crime to browse federal tax data without a business need.

Penalties Include:

- A fine not exceeding \$1,000, imprisonment of not more than one year, or both.
- Cost of prosecution.



Department of
Taxation and Finance

HELP COURSE MAP EXIT 40
of 54

Law

Federal Penalties, continued...

Federal Law, Section 7431, allows an affected taxpayer the right to file a civil lawsuit against you for browsing or for unauthorized disclosure (UNAX).

Definition:

UNAX: Willful, unauthorized inspection, access or browsing of federal tax information.



Law

Federal Penalties, continued...

Federal Law, Section 7431, allows an affected taxpayer the right to file a civil lawsuit against you for browsing or for unauthorized disclosure (UNAX).

Definition:

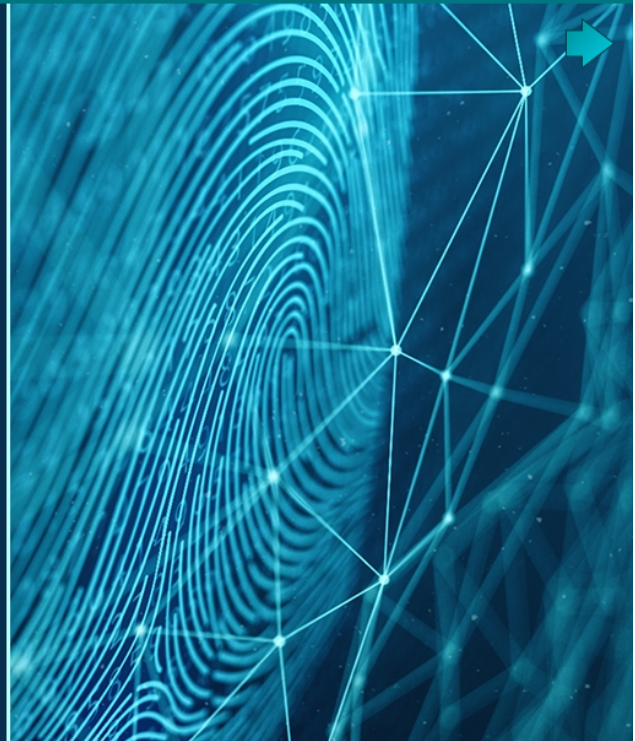
UNAX: Willful, unauthorized inspection, access or browsing of federal tax information.

Law

Office of Internal Affairs:

Between 2014 and 2023, the Office of Internal Affairs investigated twenty-six individuals who were criminally prosecuted for unlawful accessing, computer trespassing and tax secrecy violations. Twenty-six have pled guilty, including six who pled to the violation banning them from state service for five years. These cases generally involved employees or contractors looking up family members, friends, business associates and others' confidential tax information without a legitimate business reason to do so. In March 2023, a former Tax Department employee attempted to access their tax information three times but was blocked. In May 2023, another former Tax Department employee attempted to access their tax information four times but was blocked. Both employees were terminated from the Tax Department.

In 2023, the Tax Department took administrative action against seven other employees for unauthorized access or disclosure issues.



Law

Office of Internal Affairs:

Between 2014 and 2023, the Office of Internal Affairs investigated twenty-six individuals who were criminally prosecuted for unlawful accessing, computer trespassing and tax secrecy violations. Twenty-six have pled guilty, including six who pled to the violation banning them from state service for five years. These cases generally involved employees or contractors looking up family members, friends, business associates and others' confidential tax information without a legitimate business reason to do so. In March 2023, a former Tax Department employee attempted to access their tax information three times but was blocked. In May 2023, another former Tax Department employee attempted to access their tax information four times but was blocked. Both employees were terminated from the Tax Department.

In 2023, the Tax Department took administrative action against seven other employees for unauthorized access or disclosure issues.



Law Enforcement Officers

When interacting with law enforcement officers regarding taxpayer threats of assault or suicide, you must remain aware of possible disclosure concerns.

DO NOT disclose or allow access to any tax returns or return information.

If law enforcement officers ever request sensitive or confidential information – such as returns or return information:

DO:

- Immediately notify your supervisor(s)
- Contact the Department's Office of Counsel for guidance regarding the tax secrecy constraints on our ability to comply with such requests.



Law Enforcement Officers


When interacting with law enforcement officers regarding taxpayer threats of assault or suicide, you must remain aware of possible disclosure concerns.

DO NOT disclose or allow access to any tax returns or return information.

If law enforcement officers ever request sensitive or confidential information – such as returns or return information:

DO:

- Immediately notify your supervisor(s)
- Contact the Department's Office of Counsel for guidance regarding the tax secrecy constraints on our ability to comply with such requests.


 **Department of
Taxation and Finance**

HELP COURSE MAP EXIT 43
of 54

Law Enforcement Officers

When law enforcement officers are near tax information:

- Lock your computer screen
- Cooperate with the law enforcement officer
- Provide information such as name, address, phone number, and date of birth that a taxpayer verbally provided during a call or incident
- Describe any threatening words or actions of the taxpayer



Law Enforcement Officers

When law enforcement officers are near tax information:

- Lock your computer screen
- Cooperate with the law enforcement officer
- Provide information such as name, address, phone number, and date of birth that a taxpayer verbally provided during a call or incident
- Describe any threatening words or actions of the taxpayer



KNOWLEDGE CHECK

1. I received a call from a taxpayer who threatened to harm themselves. When the police come to question me it is okay for me to:
 - ☐ A. Let the police officer take a picture of my eMPIRE screen with the taxpayer's address.
 - ☐ B. Give the police officer a copy of the taxpayer's most recently filed tax return.
 - ☐ C. Give the officer the taxpayer's phone number provided during the call and explain the taxpayer's threat.
 - ☐ D. None of the above.
2. As I am packing up to leave for the day, I notice a folder containing Federal and Tax Information (FTI) is on my desk. Before leaving, I am required to:
 - ☐ A. Leave the folder in my unlocked desk drawer
 - ☐ B. Leave the folder in my locked desk drawer or in a locked filing cabinet
 - ☐ C. Throw the folder in the garbage since it is no longer needed
 - ☐ D. Leave the folder on my desk so it is easily accessible the next day

KNOWLEDGE CHECK

1. I received a call from a taxpayer who threatened to harm themselves. When the police come to question me it is okay for me to:

- A. Let the police officer take a picture of my eMPIRE screen with the taxpayer's address.
- B. Give the police officer a copy of the taxpayer's most recently filed tax return.
- C. Give the officer the taxpayer's phone number provided during the call and explain the taxpayer's threat.
- D. None of the above.

You answered the question incorrectly. You should never provide tax returns or return information without first consulting your supervisors and the Office of Counsel.

2. As I am packing up to leave for the day, I notice a folder containing Federal and Tax Information (FTI) is on my desk. Before leaving, I am required to:

- A. Leave the folder in my unlocked desk drawer
- B. Leave the folder in my locked desk drawer or in a locked filing cabinet
- C. Throw the folder in the garbage since it is no longer needed
- D. Leave the folder on my desk so it is easily accessible the next day

You answered the question incorrectly. Whenever employees are away from their desks, all FTI must be secured. If you no longer need the FTI, it must be placed in a locked controlled destruction bin for proper destruction.



KNOWLEDGE CHECK

3. Under federal law, if you are fined or imprisoned for browsing or for the unauthorized disclosure of IRS information, no civil lawsuit can be brought against you.
 - ☐ A. True
 - ☐ B. False
4. UNAX refers to the unauthorized browsing or accessing of confidential federal tax information and it is a crime.
 - ☐ A. True
 - ☐ B. False
5. My co-worker and I continued a conversation about a confidential matter after leaving the conference room. This is okay because we are in a secure building.
 - ☐ A. True
 - ☐ B. False

KNOWLEDGE CHECK

3. Under federal law, if you are fined or imprisoned for browsing or for the unauthorized disclosure of IRS information, no civil lawsuit can be brought against you.

A. True

You answered the question incorrectly. Under federal law, not only can you be fined or imprisoned for browsing or for the unauthorized disclosure of IRS information, but the taxpayer can also file a civil lawsuit against you.

B. False

4. UNAX refers to the unauthorized browsing or accessing of confidential federal tax information and it is a crime.

A. True

B. False

You answered the question incorrectly. It is a crime to browse Federal Tax Information.

5. My co-worker and I continued a conversation about a confidential matter after leaving the conference room. This is okay because we are in a secure building.

A. True

You answered the question incorrectly. Conversations about confidential information should be held in private with only those who have a need to know.

B. False



KNOWLEDGE CHECK

6. I receive a call from another agency saying their system is down and they need some information immediately. They want me to provide them with taxpayer information. I am not exactly sure who the person is but I am always happy to help out another agency. It's okay to provide them with the information they are looking for.
- ☐ A. True
 - ☐ B. False
7. You observe a colleague on his laptop posting confidential tax information on Facebook about different taxpayers. In this situation you must:
- ☐ A. Do nothing. Confidential information posted by my colleague on Facebook is not my concern.
 - ☐ B. Call the taxpayer to inform them of the unauthorized disclosure of their tax information
 - ☐ C. Immediately confiscate your colleague's laptop
 - ☐ D. Immediately report the incident to the Department's Office of Internal Affairs.

KNOWLEDGE CHECK

6. I receive a call from another agency saying their system is down and they need some information immediately. They want me to provide them with taxpayer information. I am not exactly sure who the person is but I am always happy to help out another agency. It's okay to provide them with the information they are looking for.

A. True

That's not the correct answer. Scam artists may pose as Tax Department or Government employees to obtain confidential information. Please refer to your supervisor or contact the Disclosure Office before disclosing any information.

B. False

7. You observe a colleague on his laptop posting confidential tax information on Facebook about different taxpayers. In this situation you must:

- A. Do nothing. Confidential information posted by my colleague on Facebook is not my concern.
- B. Call the taxpayer to inform them of the unauthorized disclosure of their tax information
- C. Immediately confiscate your colleague's laptop

That's not the correct answer. All Department employees are to report any work-related incident that they believe constitutes an information security breach or unauthorized disclosure of confidential tax information or private information.

D. Immediately report the incident to the Department's Office of Internal Affairs.



KNOWLEDGE CHECK

8. I am currently auditing a high-profile taxpayer and have access to their tax information. The woman sitting next to me has no business need to know this information. It is ok to for me to show her this tax information since we are both New York State employees.
- ☐ A. True
 - ☐ B. False
9. I need to send paper Federal Tax Information (FTI) to the Tax Department's Buffalo District Office from Albany. I can use a single, standard envelope to mail the FTI.
- ☐ A. True
 - ☐ B. False

KNOWLEDGE CHECK

8. I am currently auditing a high-profile taxpayer and have access to their tax information. The woman sitting next to me has no business need to know this information. It is ok to for me to show her this tax information since we are both New York State employees.

A. True
B. False

That's not the correct answer. You cannot disclose any information about this taxpayer unless: (1) You are authorized to disclose the information and (2) the person(s) you are disclosing to are authorized employees with a business need to know.

9. I need to send paper Federal Tax Information (FTI) to the Tax Department's Buffalo District Office from Albany. I can use a single, standard envelope to mail the FTI.

A. True
B. False

That's not the correct answer. Federal Tax Information sent to another location must be double sealed (one envelope inside another envelope).



KNOWLEDGE CHECK

10. Under Section 7213 of the Internal Revenue Code, an individual who is found guilty of making unauthorized disclosure of Federal Tax Information could face:
- ☐ A. A misdemeanor, a fine up to \$100, up to 6 months in jail, or both.
 - ☐ B. A misdemeanor, a fine up to \$1,000, up to 1 year in prison, or both. | Cost of Prosecution. | Possible Disciplinary Action.
 - ☐ C. A felony, a fine up to \$5,000, up to 5 years in prison, or both. | Cost of Prosecution. | Possible Disciplinary Action.
 - ☐ D. A felony, a fine up to \$10,000, up to 5 years in prison, or both. | Cost of Prosecution. | Possible Disciplinary Action.

KNOWLEDGE CHECK


10. Under Section 7213 of the Internal Revenue Code, an individual who is found guilty of making unauthorized disclosure of Federal Tax Information could face:
- A. A misdemeanor, a fine up to \$100, up to 6 months in jail, or both.
 - B. A misdemeanor, a fine up to \$1,000, up to 1 year in prison, or both. | Cost of Prosecution. | Possible Disciplinary Action.
 - C. A felony, a fine up to \$5,000, up to 5 years in prison, or both. | Cost of Prosecution. | Possible Disciplinary Action.
 - D. A felony, a fine up to \$10,000, up to 5 years in prison, or both. | Cost of Prosecution. | Possible Disciplinary Action.

KNOWLEDGE CHECK

11. Bill, a New York State Tax Department employee observes his coworker, Jane accessing Federal Tax Information for a high profile taxpayer. Jane tells Bill that she does not have a case assigned to him for the taxpayer. She says she was curious to know how much income the taxpayer reported on their tax return. How should Bill report this incident?
- ☐ A. He does not need to report anything since it really does not concern him.
 - ☐ B. He should wait until the end of the week and then call the IRS to report the incident.
 - ☐ C. He should report the incident to the Office of Internal Affairs via email at DTFOIA@tax.ny.gov or by calling them at (518) 451-1566.
 - ☐ D. He should tell Jane to stop illegally accessing tax information and report the incident to her supervisor.

KNOWLEDGE CHECK

11. Bill, a New York State Tax Department employee observes his coworker, Jane accessing Federal Tax Information for a high profile taxpayer. Jane tells Bill that she does not have a case assigned to him for the taxpayer. She says she was curious to know how much income the taxpayer reported on their tax return. How should Bill report this incident?
- A. He does not need to report anything since it really does not concern him.
 - B. He should wait until the end of the week and then call the IRS to report the incident.
 - C. He should report the incident to the Office of Internal Affairs via email at DTFOIA@tax.ny.gov or by calling them at (518) 451-1566.
 - D. He should tell Jane to stop illegally accessing tax information and report the incident to her supervisor.



Department of
Taxation and Finance

HELP

COURSE
MAP

EXIT

50
of 54

Frequently Asked Questions

Federal Tax Information Part 1:


Question: FTI obtained from e-MPIRE is written down on a separate piece of paper. Do I need to log this somewhere?

Answer: The information should be clearly labeled as Federal Tax Information and you need to keep a log of this information just like you would if you printed FTI.

Inadvertent Unauthorized Disclosure Part 1:

Question: What happens if, when accessing DTF computerized files, I make a typing error and end up pulling up a non-assigned case. Will I be accused of a UNAX violation?

Answer: No, accesses resulting from a typing error are **NOT** UNAX violations. A UNAX violation requires willful unauthorized access. Inadvertent or mistaken accesses are **NOT** violations of the law. This access should be noted in your access log with a note stating the circumstances.



Frequently Asked Questions

Federal Tax Information Part 1:

Question: FTI obtained from e-MPIRE is written down on a separate piece of paper. Do I need to log this somewhere?

Answer: The information should be clearly labeled as Federal Tax Information and you need to keep a log of this information just like you would if you printed FTI.

Inadvertent Unauthorized Disclosure Part 1:

Question: What happens if, when accessing DTF computerized files, I make a typing error and end up pulling up a non-assigned case. Will I be accused of a UNAX violation?

Answer: No, accesses resulting from a typing error are **NOT** UNAX violations. A UNAX violation requires willful unauthorized access. Inadvertent or mistaken accesses are **NOT** violations of the law. This access should be noted in your access log with a note stating the circumstances.



Comments and Suggestions

This training will be updated each year. If you would like a topic or have a question you would like addressed, please e-mail your comments or suggestions to the IRS Compliance Mailbox:

Tax.dl.IRSComplianceUnit

Comments and Suggestions

This training will be updated each year. If you would like a topic or have a question you would like addressed, please e-mail your comments or suggestions to the IRS Compliance Mailbox:

Tax.dl.IRSComplianceUnit



DTF- 202



- **DTF-202:** Tax Information Access and Non-Disclosure Agreement

- **Important:**

Non- DTF Employees are required to read and agree to the secrecy provisions that are contained in the [DTF-202](#).



DTF- 202

- **DTF-202:** Tax Information Access and Non-Disclosure Agreement

- **Important:**

Non- DTF Employees are required to read and agree to the secrecy provisions that are contained in the [DTF-202](#).

Acknowledgement

By completing this training, I acknowledge that:

Please place a check mark in each of the boxes below by clicking each box to accept the corresponding statement.

I understand the concepts provided within the training.

I understand that the unauthorized access, disclosure and/or acquisition of confidential information is a crime.

I agree never to view any confidential information that is not part of my regular job responsibilities.

I have read the provisions in the ***Public Officers Law*** ([Section 73](#) and [Section 74](#) provisions for all state officers, employees and party officers).

I have read the [DTF 202, Tax Information Access and Non-Disclosure Agreement](#) (For Contractors and other Non-DTF employees).

Print name

Signature

Date

Email address