



Department of
Taxation and Finance

2022 Annual Access and Disclosure Training for Non-Tax Employees

[Get Started](#) ►



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:

- 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.



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

Knowledge Check

1. Information system design documentation is confidential

True

False - You answered the question incorrectly. Information system design documentation IS confidential.

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

True - You answered the question incorrectly. It is NEVER ok to access one's own tax records.

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.

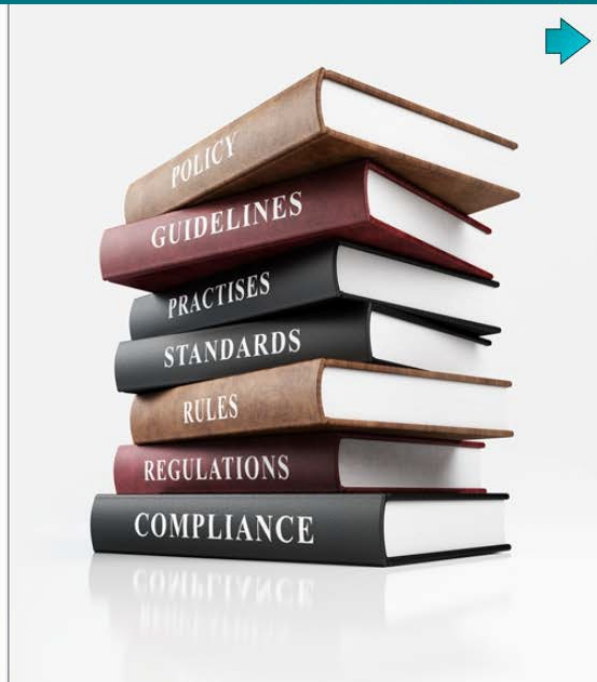
True You answered the question incorrectly. Information should only be accessed on a "Need to Know" basis. It is a coworker asking without a reason and not a supervisor who articulates business reason for making the access.

False



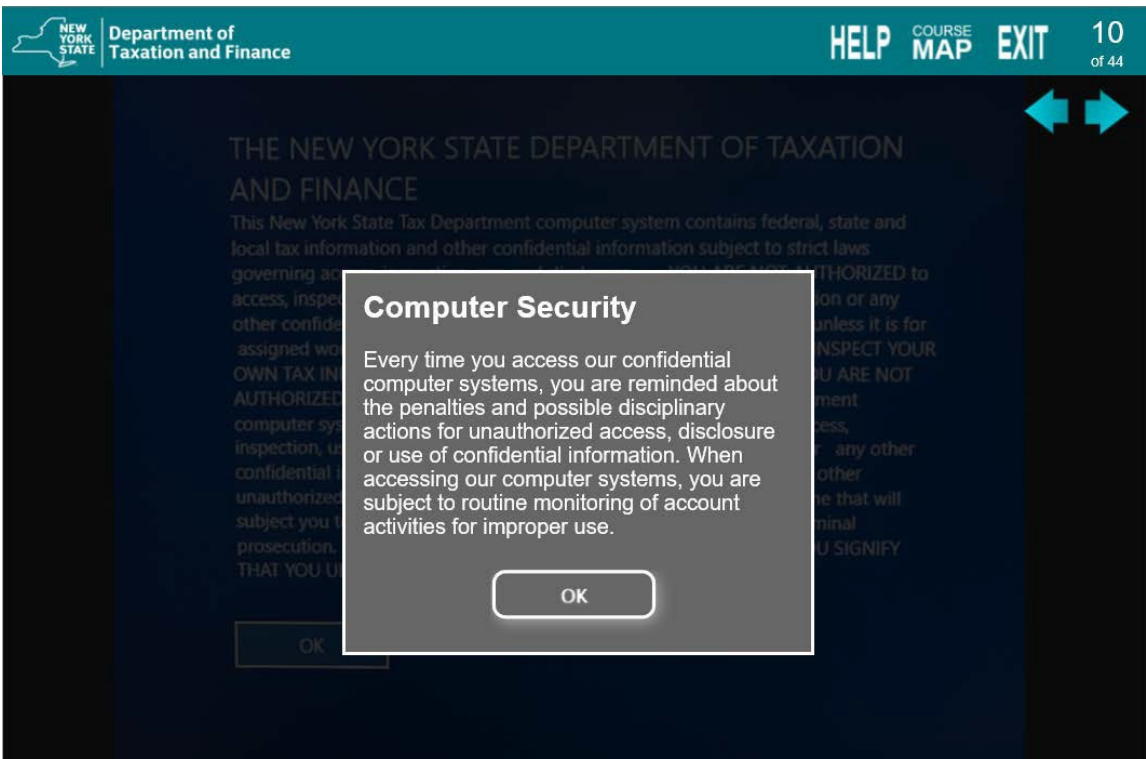
Public Officers Law

[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.



THE NEW YORK STATE DEPARTMENT OF TAXATION AND FINANCE

This New York State Tax Department computer system contains federal, state and local tax information and other confidential information subject to strict laws governing access, inspection, use and disclosure. - YOU ARE NOT AUTHORIZED to access, inspect, use or disclose any federal, state or local tax information or any other confidential information on the Department's computer system unless it is for assigned work duties. - THERE IS NEVER A REASON TO ACCESS OR INSPECT YOUR OWN TAX INFORMATION OR THAT OF ANY FAMILY MEMBER AND YOU ARE NOT AUTHORIZED TO DO SO. - Your use of this computer and the Department computer system is being logged and monitored. - Unauthorized access, inspection, use or disclosure of federal, state or local tax information or any other confidential information on the Department's computer system or any other unauthorized use of the Department's computer system may be a crime that will subject you to disciplinary action and federal and/or state civil and criminal prosecution. - For information see E-memo 141. BY LOGGING IN, YOU SIGNIFY THAT YOU UNDERSTAND AND AGREE WITH THIS NOTICE.

OK

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 write your PASSWORD down.
- 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 write your PASSWORD down.
- Do NOT use the same PASSWORD for different systems (e.g. home PC, personal e-mail account, personal bank account, etc...)



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"



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"



Computer Security



Security Guidelines for DTF 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.

DO NOT install unapproved files or software on your computer.

Computer Security

Security Guidelines for DTF 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.

DO NOT install unapproved files or software on your computer.

KNOWLEDGE CHECK



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.

- True
- 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.

- True
- False

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."

- True
- False

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.

True

False

You answered the question incorrectly. 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.

True

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

False

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."

True

You answered the question incorrectly. You must click "no," "not for this site," or "never for this website" when a pop-up appears asking you to store your password.

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.

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.

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.

Definition:

Unauthorized Disclosure: Knowingly 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

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.

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.

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.

Definition:

Unauthorized Disclosure: Knowingly 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

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.

Information Protection

Properly Dispose of Confidential Information:

You must shred confidential paper documents using a Department approved shredder, or you may place them in a locked confidential destruction bin where available. Do **NOT** place any papers containing confidential information in the trash, recycling (3R's) baskets or in open gondolas.

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.

To view a copy of the **Electronic Media Disposal Policy** or any related questions, please contact OSB at tax.sm.OSB.Support.Services.



Information Protection

Properly Dispose of Confidential Information:

You must shred confidential paper documents using a Department approved shredder, or you may place them in a locked confidential destruction bin where available. Do **NOT** place any papers containing confidential information in the trash, recycling (3R's) baskets or in open gondolas.

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.

To view a copy of the **Electronic Media Disposal Policy** or any related questions, please contact OSB at tax.sm.OSB.Support.Services.

"Access Denied" Error Message



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 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 for an 'Individual Taxpayer Profile Inquiry'. The page has a navigation bar with 'Client Information', 'Account Information', 'Work Management', and 'Special Services'. Below the navigation bar, there are fields for 'ID:', 'Name:', and 'Address:', and 'Associated ID:' and 'Associated Name:'. A search bar is visible with a dropdown menu set to '9 Character ID' and the value '123456789'. Below the search bar, there is a red error message: '! S06527 ACCESS DENIED: See Executive Memorandum E-141. Contact your supervisor now'. The page also includes a 'Taxpayer Summary' section and several icons in the bottom right corner.

"Access Denied" Error Message

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 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.

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).

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 are available from the Disclosure Unit located in Bldg. 8, Room 700.

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 are available from the Disclosure Unit located in Bldg. 8, Room 700.

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
(Rev. 12-97)
Internal Revenue Service

Notice 129A

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.

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.



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



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.

Law



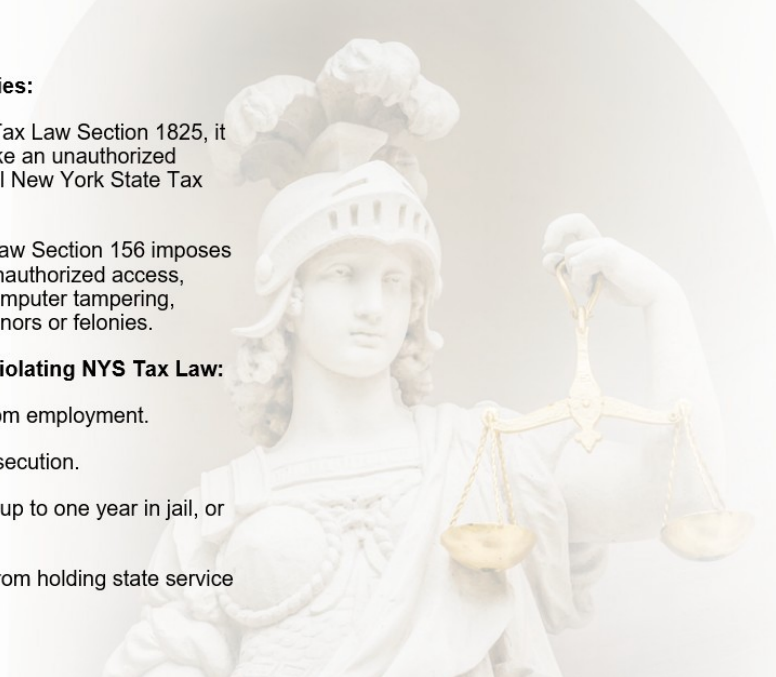
New York State Penalties:

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.

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.



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 2019, the Office of Internal Affairs investigated 23 individuals who were criminally prosecuted for unlawful accessing, computer trespassing and tax secrecy violations. All 23 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 2019, the Tax Department terminated two employees for attempting to look up their own tax information. Additionally, the Tax Department took administrative action against seven other employees for unauthorized access or disclosure issues.



Law

Office of Internal Affairs:

Between 2014 and 2019, the Office of Internal Affairs investigated 23 individuals who were criminally prosecuted for unlawful accessing, computer trespassing and tax secrecy violations. All 23 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 2019, the Tax Department terminated two employees for attempting to look up their own tax information. Additionally, 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.

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:
- Let the police officer take a picture of my eMPIRE screen with the taxpayer's address.
 - Give the police officer a copy of the taxpayer's most recently filed tax return.
 - Give the officer the taxpayer's phone number provided during the call and explain the taxpayer's threat.
 - 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:
- Leave the folder in my unlocked desk drawer
 - Leave the folder in my locked desk drawer or in a locked filing cabinet
 - Throw the folder in the garbage since it is no longer needed
 - 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:

- Let the police officer take a picture of my eMPIRE screen with the taxpayer's address.

You answered the question incorrectly. You should lock your computer screens when law enforcement officials are nearby. And you should not provide any tax returns or return information (including return information from eMPIRE screens) without first consulting your supervisors and the Office of Counsel.

- Give the police officer a copy of the taxpayer's most recently filed tax return.

You answered the question incorrectly. You should never

provide tax returns or return information without first consulting your supervisors and the Office of Counsel.

- Give the officer the taxpayer's phone number provided during the call and explain the taxpayer's threat.
- 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:

Leave the folder in my unlocked desk drawer

Leave the folder in my locked desk drawer or in a locked filing cabinet

Throw the folder in the garbage since it is no longer needed

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



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.

- True
- False

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

- True
- 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.

- True
- False

6. 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.

- True
- 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.

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

False

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

True

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.

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

False

6. 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.

True - The answer is False – 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.

False



KNOWLEDGE CHECK

7. 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.

- True
- False

8. 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.

- True
- False

KNOWLEDGE CHECK

7. 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.

True - You answered the question incorrectly. 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.

False

8. 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.

True - The answer is False - Federal Tax Information sent to another location must be double sealed (one envelope inside another envelope).

False

KNOWLEDGE CHECK

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

- Do nothing. Confidential information posted by my colleague on Facebook is not my concern
- Call the taxpayer to inform them of the unauthorized disclosure of their tax information
- Immediately confiscate your colleague's laptop
- Immediately report the incident to the Department's Office of Internal Affairs.

KNOWLEDGE CHECK

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

Do nothing. Confidential information posted by my colleague on Facebook is not my concern - You answered the question incorrectly. Under New York State Law, it is unlawful for you to disclose confidential information outside of the Department. You can be fined or imprisoned for the unauthorized disclosure of the information along with the possible dismissal from employment.

Call the taxpayer to inform them of the unauthorized disclosure of their tax information - You answered the question incorrectly. Under New York State Law, it is unlawful for you to disclose confidential information outside of the Department. You can be fined or imprisoned for the unauthorized disclosure of the information along with the possible dismissal from employment.

Immediately confiscate your colleague's laptop - You answered the question incorrectly. Under New York State Law, it is unlawful for you to disclose confidential information outside of the Department. You can be fined or imprisoned for the unauthorized disclosure of the information along with the possible dismissal from employment.

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

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?

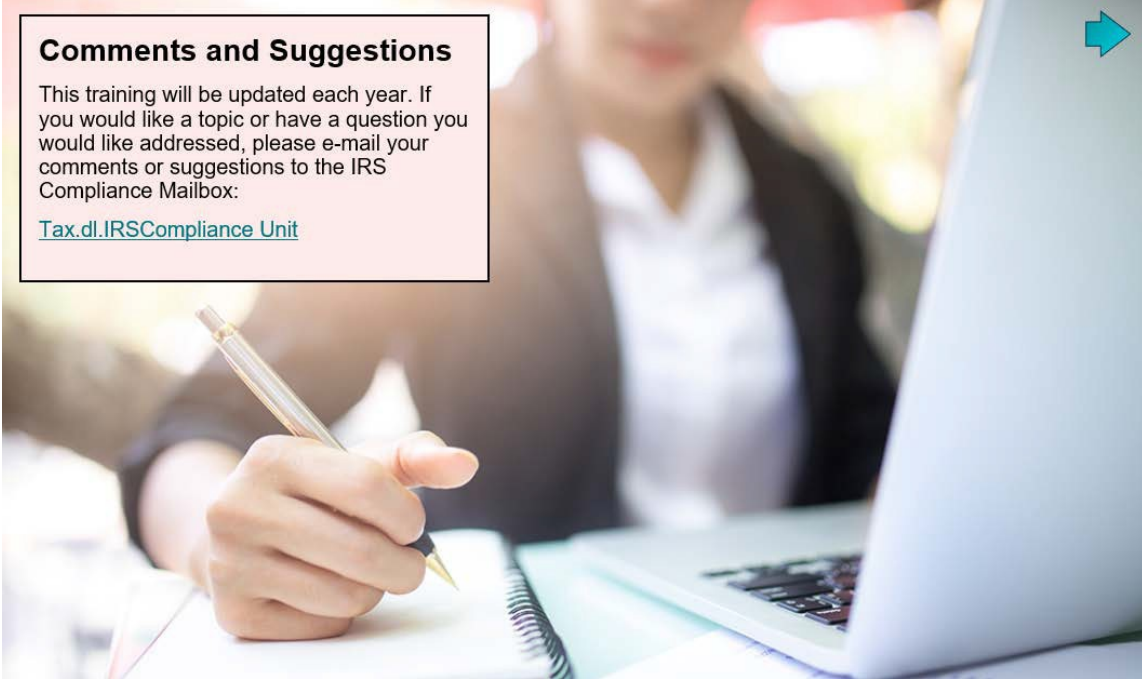
Answer: No, accesses resulting from a typing error are **NOT** UNAX violations. A UNAX violation requires willful unauthorized access. Inadvertent or mistaken accesses are **NOT** violations of the law. This access should be noted in your access log with a note stating the circumstances.



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.IRSCompliance Unit



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.IRSCompliance Unit



DTF- 202

- **DTF-202:** Agreement to Adhere to the Secrecy Provisions of the Tax Law and the Internal Revenue Code
- **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
