

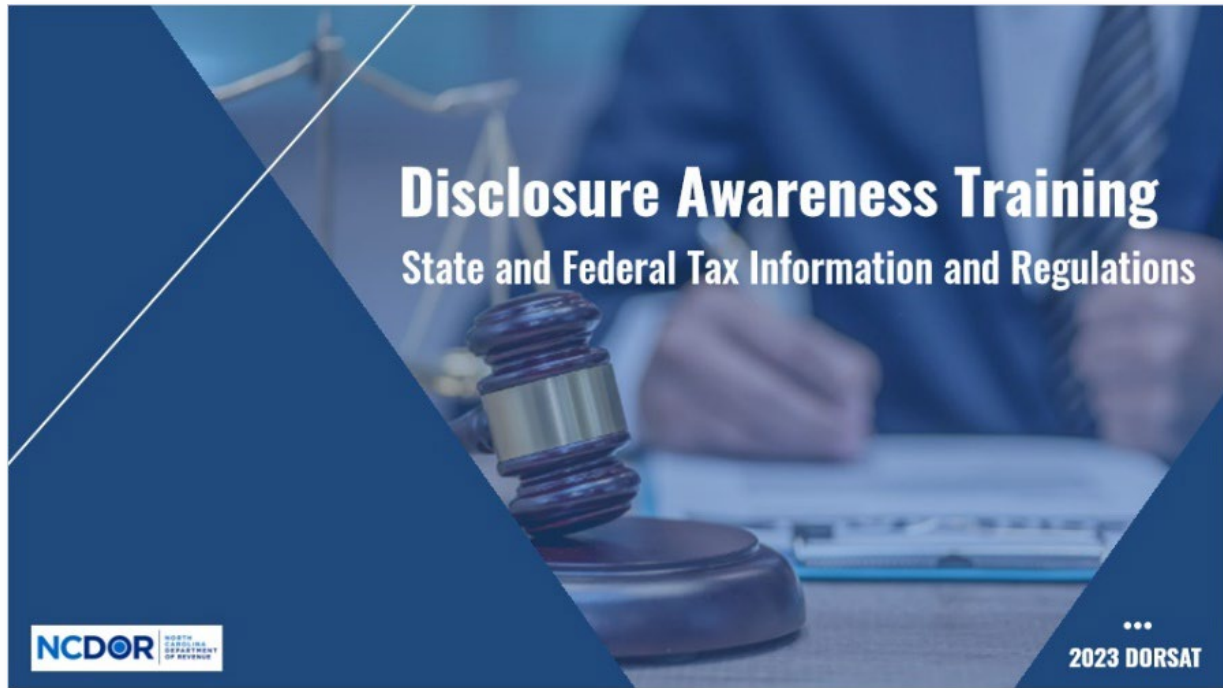
2023 DORSAT Annual DOR Security Awareness Training



Table of Contents

SECTION 1: State and Federal Tax Information and Regulations	3
SECTION 2: Staff Security Responsibilities and Facility Security Reminders	43

SECTION 1: State and Federal Tax Information and Regulations



Slide Notes

Welcome to State and Federal Tax Information and Regulations. This section will review the importance of protecting taxpayer information entrusted to us by the people of North Carolina.

Learning Objectives

01

List and define the data classifications at Revenue

02

Define Federal Tax Information (FTI) and federal regulations

03

Describe how Federal Tax Information is used at Revenue

04

Recognize how to protect Federal Tax Information

05

Identify types of confidential data

06

Explain state law relating to taxpayer information

Slide Notes

At the conclusion of this eModule, you will be able to:

- List and define the data classifications at Revenue
- Define Federal Tax Information (FTI) and federal regulations
- Describe how Federal tax Information is used at Revenue
- Recognize how to protect Federal Tax Information
- Identify types of confidential data
- Explain state law relating to taxpayer information

Data Classifications



The slide displays four data classification categories in a 2x2 grid. Each category is represented by a small image with a title above it: 'Federal Tax Information' (tax forms and pen), 'Confidential Information' (blue digital data with a padlock), 'Public Information' (laptop and smartphone), and 'All Possible' (hands typing on a laptop keyboard with data visualizations).

All Possible, Federal Tax Information, and Confidential Information should be protected and handled with care.

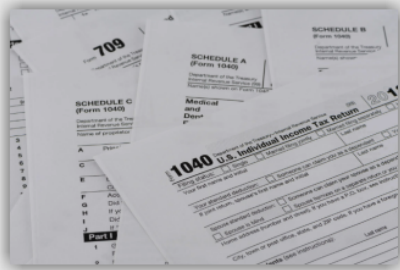
Slide Notes

The four data classifications used at Revenue are:

- Federal Tax Information
- Confidential Information
- Public Information
- All Possible

All Possible, Federal Tax Information, and Confidential Information should be protected and handled with care.

What is Federal Tax Information or FTI?



Federal Tax Information consists of federal tax returns and return information and information derived from it that is in the agency's possession or control and is covered by the confidentiality protections of the IRC (Internal Revenue Code).

Slide Notes

Federal Tax Information consists of federal tax returns and return information and information derived from it that is in the agency 's possession or control that is covered by the confidentiality protections of the IRC (Internal Revenue Code) and subject to IRC 6103 (p)(4) safeguarding requirements, including IRS oversight.

Sensitive But Unclassified (SBU)



FTI is defined by the IRS as Sensitive But Unclassified information (SBU) and may contain Personally Identifiable Information (PII).



FTI includes any information created by the recipient that is derived from a federal return.

Slide Notes

FTI is categorized by the IRS as Sensitive but Unclassified information (SBU) and may contain personally identifiable information (PII).

FTI includes any information created by the recipient that is derived from a federal return or return information received from the IRS or obtained through a secondary source.



Slide Notes

FTI may include the following PII elements:

- Name of a person with respect to whom a return is filed
- Taxpayer mailing address
- Taxpayer identification number
- Email addresses
- Telephone numbers
- Social security number
- Bank account numbers
- Date and place of birth
- Mother's maiden name
- Biometric data (e.g., height, weight, eye color, fingerprints)
- Any combination of the above



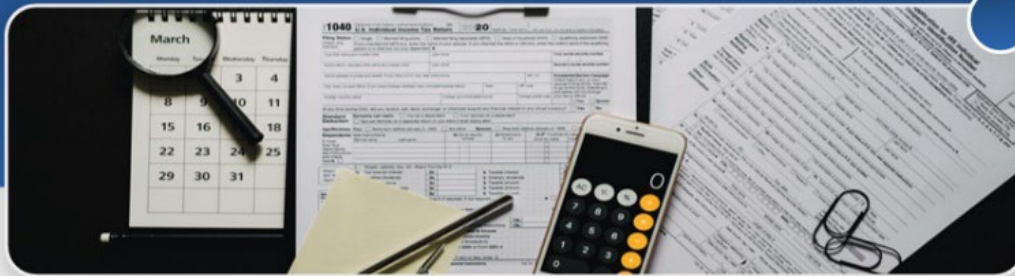
What is a return and return information?

A return is any tax or information return, estimated tax declaration, or refund claim (e.g., amendments, supplements, supporting schedules, attachments, or lists).

Slide Notes

A return is any tax or information return, estimated tax declaration, or refund claim (including amendments, supplements, supporting schedules, attachments, or lists) required by or permitted under the IRC and filed with the IRS by, on behalf of, or with respect to any person or entity.

Return Examples



Forms filed on paper or electronically (e.g., forms 1040, 941, and 1120) and any informational forms (e.g., 1099 or W-2).

Forms include supporting schedules and attachments or lists that are supplemental to or part of such a return.

Return Information

Return information is any information collected or generated by the IRS regarding any person's liability or possible liability under the IRC.



Slide Notes

Return information is any information collected or generated by the IRS regarding any person's liability or possible liability under the IRC. IRC 6103(b)(2)(A) defines return information very broadly. It includes but is not limited to:

- Information that the IRS obtained from any source or developed through any means that relates to the potential liability of any person under the IRS for any tax, penalty, interest, fine, forfeiture, or other imposition or offense.
- Information extracted from a return, including names of dependents or the location of business.
- Information collected by the IRS about any person's tax affairs, even if identifiers, such as name, address, and identification number are deleted.
- Status of whether a return was filed, under examination or subject to other investigation or processing, including collection activities.
- Information contained on transcripts of accounts.

Disclosures under Internal Revenue Code Section 6103

Within the Internal Revenue Code Section 6103, it states that Federal Tax information may be disclosed to:



Actual
Taxpayer



Taxpayer's
Designee



State Tax
Official



Other
Person

If you have questions regarding who you are able to disclose tax information to, please contact your supervisor.

Slide Notes

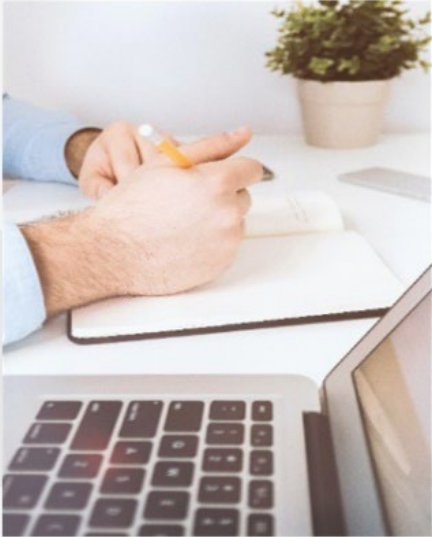
Within Internal Revenue Code Section 6103, it states that Federal Tax Information may be disclosed to:

- The actual taxpayer of the tax return and return information
- The taxpayer's designee, provided a Power of Attorney has been provided for this person from the taxpayer
- State Tax officials, including Revenue staff, with a business need to use information for tax administration purposes (*IRC 6103(d)*)
- Other persons, such as law enforcement or authorized third parties, who are authorized for the purposes of administering the state tax law and have a business need for the information

If you have questions regarding who you are able to disclose tax information to, please contact your supervisor.

Internal Revenue Service and Revenue Information Sharing

The Internal Revenue Service and the Department of Revenue share information regarding North Carolina taxpayers.



- Update our income master file
- Identify any persons or companies who did not file
- Identify sources of income

All of this helps our agency recover lost revenue owed to our State.


Slide Notes

The Internal Revenue Service and the Department of Revenue share information regarding North Carolina taxpayers.

Revenue uses this information to:



- Update our income tax master file, including taxpayer names, addresses, and deceased data.
- Identify any persons or companies who did not file, referred to as non-filing taxpayers for North Carolina and to identify taxpayers who underreported their income.
- Identify sources of income which may be used for state tax collection activities.

All of this helps our agency recover lost revenue owed to our State.



Federal Tax Information (FTI) - Copying Data

Agency employees often forget that information derived from FTI is considered federal tax information and must be safeguarded.




Remembering these concepts will ensure that all FTI data is properly safeguarded.

Slide Notes

Agency personnel often forget that information derived from FTI is considered federal taxpayer information and must be safeguarded.

- Derived FTI includes things like photocopies, scanned data, or information transcribed into a form, letter, application, or spreadsheet.
- **Example:** Writing information from FTI on a sticky note for quick reference. The sticky note then becomes FTI, which requires safeguarding.

Remembering these concepts will ensure that all FTI data is properly safeguarded.



DOR, FTI, and Regulations


- Revenue generates millions of dollars in increased collections based on information received from the Internal Revenue Service.
- Most of the income surplus our agency has goes back to the state legislature.
- In order to keep receiving information from the Internal Revenue Service, we're required to adhere to federal laws and regulations.

Slide Notes

During an average fiscal year, Revenue generates millions of dollars in increased collections based on information received from the Internal Revenue Service.

Since most of the income surplus our agency has goes back to the state legislature, which in turn distributes it to other state agencies via budget allocations, it helps the entire state.

In order to keep receiving information from the Internal Revenue Service, we're required to adhere to federal laws and regulations. These include Internal Revenue Service Publication 1075 and the Internal Revenue Code sections that are covered later in this training.



Commingled Data

Commingling of FTI refers to having FTI and non-FTI data stored together.

Federal taxpayer information combined with state tax information is referred to as commingled data.	Commingled data must be safeguarded as required by federal law.
Commingling of federal and state tax information subjects the entire file to safeguard requirements.	Commingled data must be clearly labeled to indicate that FTI is included.

Slide Notes

Commingling of FTI refers to having FTI and non-FTI data stored together, regardless of format.

- Federal taxpayer information combined with state tax information is considered as commingled data.
- Commingling of Federal and State Tax Information subjects the entire file to the safeguard requirements mandated by the IRS.
- Commingled data must be safeguarded as required by federal law from unauthorized access, disclosure, and inspection.
- Commingled data must be clearly labeled to indicate that FTI is included, and the file must be safeguarded.

Protection of Commingled Data



To safeguard FTI or commingled data, you should never access or attempt to access taxpayer information for any of the following reasons:

- To satisfy a curiosity
- For personal use
- To look up or attempt to modify account information

Looking up a prior case that is no longer assigned to you is considered accessing it without a business need.

If you are assigned an audit or receive tax information for someone that you have a personal relationship with or know on a personal level as part of your job assignments, you should notify your supervisor immediately.

Confidential Data

Now that we have defined Federal Taxpayer Information and federal regulations, let's identify the different types of confidential data that we must protect.

Confidential data requires protection and proper destruction. It is important to understand what types of data are considered as confidential.



Slide Notes

Now that we have defined Federal Taxpayer Information and Federal Regulations, let's identify the different types of confidential data that we must protect.

Confidential data requires protection and proper destruction. It is important to understand what types of data are considered as confidential.

Confidential data includes:

- Personal information which is also referred to as Personally Identifiable Information as defined in NC G.S. 75-61.10
- Merchant Credit Card Data
- State Taxpayer Information as defined in NC G.S. 105-259(b)
- User Passwords

Other types of Confidential Data

- Information system security data such as security configuration settings
- Detailed plans and drawings of public buildings and infrastructure facilities
- Contract bids and contract bid proposals
- Information provided by other state agencies



Slide Notes

Other types of confidential data include but are not limited to:

- Information system security data such as security configuration settings and other data about the security of our systems.
- Detailed plans and drawings of public buildings and infrastructure facilities.
- Contract bids and contract bid proposals that include identified vendor trade secrets.
- Information provided by other state agencies for tax administration purposes.

Reporting Improper Inspections or Disclosures



A data incident is an occurrence that:

- actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information
- constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies

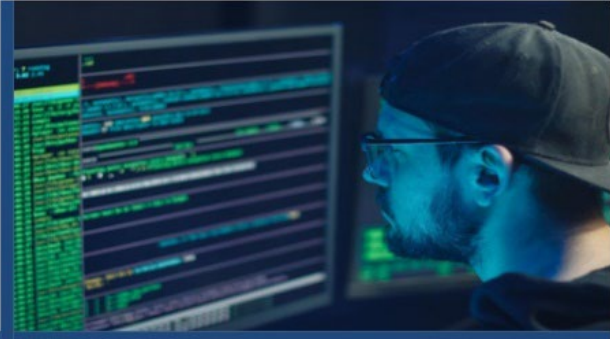
Slide Notes

A data incident is an occurrence that:

- actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of information or an information system; or
- constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies. Incidental and inadvertent accesses are considered data incidents.

What is a Data Breach?

A data breach is a type of incident involving a loss, theft, or inadvertent disclosure of FTI. A data breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:



- a person other than an authorized user accesses or potentially accesses FTI
- an authorized user accesses or potentially accesses FTI for an unauthorized purpose

Common Examples of a Data Breach

- A laptop or portable storage device storing FTI is lost or stolen
- An email containing FTI is inadvertently sent to the wrong person
- A box of documents with FTI is lost or stolen during shipping
- An unauthorized third party overhears agency employees discussing FTI
- A user with authorized access to FTI sells it for personal gain or disseminates it
- An IT system that maintains FTI is accessed by a malicious actor
- FTI is posted inadvertently on a public website



Data Breach Occurrences

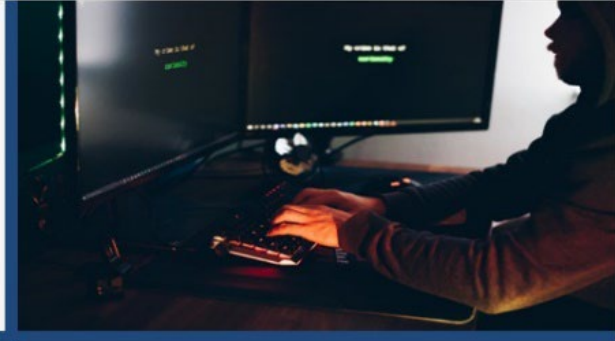
A **data breach** is not limited to an occurrence where:

- a person other than an authorized user potentially accesses FTI by means of a network intrusion
- a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment



Data Breach Occurrences

- the loss or theft of physical documents that include FTI and portable electronic storage media that store FTI
- the inadvertent disclosure of FTI on a public website



- an oral disclosure of FTI to a person who is not authorized to receive that information
- an authorized user accessing FTI for an unauthorized purpose

Slide Notes

A data breach may also include:

- the loss or theft of physical documents that include FTI and portable electronic storage media that store FTI
- the inadvertent disclosure of FTI on a public website
- an oral disclosure of FTI to a person who is not authorized to receive that information
- It may also include an authorized user accessing FTI for an unauthorized purpose

Incident Reporting

Upon discovering a possible improper inspection or disclosure of FTI, including breaches and incidents, by a federal employee, a state employee, or any other person...

The individual making the observation or receiving the information should report the suspected or actual information security incident immediately to the DOR IT Service Desk at (919) 754-2323 or email the Service Desk at ServiceDesk@ncdor.gov.

Alternatively, DOR employees can use the self-service option in ServiceNow titled **Report an IT Issue** and select Information Security Incident to report.

The DOR Disclosure Officer must report the incident to the **IRS Office of Safeguards** immediately, but no later than 24 hours after identification of a possible issue involving FTI.





FTI in Transit

- **FTI must be handled in such a way** that it does not become misplaced or available to unauthorized personnel.
- **Any time FTI is transported from one location to another,** care must be taken to provide appropriate safeguards.
- **When FTI is hand-carried by an individual** in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from unauthorized disclosure.
- **All shipments of paper or electronic FTI** including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes and microform must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.

Slide Notes

- FTI must be handled in such a way that it does not become misplaced or available to unauthorized personnel.
- Any time FTI is transported from one location to another, care must be taken to provide appropriate safeguards.
- When FTI is hand-carried by an individual in connection with a trip or in the course of daily activities, it must keep with that individual and protected from unauthorized disclosures.
- All shipments of paper or electronic FTI including compact disk [CD], digital video disk [DVD], thumb drives, hard drives, tapes, and microform must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged.

Alternate Work Sites

If the confidentiality of FTI can be adequately protected, telework sites such as employees' home or other non-traditional work site can be used.



Slide Notes

If the confidentiality of FTI can be adequately protected, telework sites such as employees' home or other non-traditional work sites can be used.

- FTI remains subject to the same safeguard requirements and the highest level of attainable security.
- The agency must retain ownership and control for all hardware, software, and end-point equipment connecting to public communication networks where these are present at alternate work sites.
- Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done.
- Employees also must have a way to communicate with their managers or other members of the agency if security problems arise.



Slide Notes

Public records may include documents, paper, email, text messages, or other means used to transact state business by any agency of the North Carolina government and are the property of the people as defined in North Carolina General Statute 132-1.

Although these records are considered public property, there are limitations.

Public records do not include confidential or protected communications as defined in NC G.S. 105-259.



North Carolina General Statute 105-259

- We may not disclose tax information to any other person unless the disclosure is specifically permitted by the statute.
- North Carolina General Statute Chapter 132 defines public records.
- If you receive a request for public records, please forward it to our Director of Public Affairs.

Slide Notes

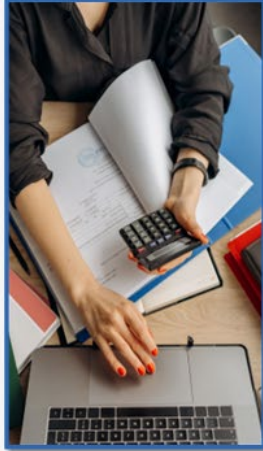
The North Carolina General Statute 105-259 also states that:

- We may not disclose tax information to any other person unless the disclosure is specifically permitted by the statute.
- NC G.S. Chapter 132 defines public records.

Therefore, if you receive a request for public records, please forward it to our Director of Public Affairs.

Protected Taxpayer Information

Taxpayer information is protected under the North Carolina General Statute 105-259.



The North Carolina General Statute applies to current and former staff and officers, as well as contractors.

Slide Notes

Taxpayer information is protected under North Carolina General Statute 105-259.

Protected tax information includes the following:

- Information on a tax return, report, or an application for a license for which a tax is imposed
- Information from an audit of a taxpayer, or correspondence with a taxpayer, or correspondence from a taxpayer
- Information about whether a taxpayer has filed a return or report
- The North Carolina General Statute applies to current and former staff and officers, as well as contractors

Unauthorized Disclosure of State Tax Information

In the event of an unauthorized disclosure of State Tax Information (STI) in regards to North Carolina General Statute 105-259, the following penalties may apply under North Carolina State law:



Slide Notes

In the event of an unauthorized disclosure of State Tax Information (STI) in regard to North Carolina General Statute 105-259, the following penalties may apply under North Carolina State law:

- Class 1 Misdemeanor
- Dismissal from Public Office
- Termination of employment without the possibility of rehire for 5 years



Incident Response Notification to Impacted Individuals

The agency must provide written notification to a taxpayer...

- whose FTI was subject to unauthorized access or disclosure when a disciplinary or adverse action is proposed against the agency employee responsible

The required written notification to the taxpayer must include:

- the date of the unauthorized inspection or disclosure and the rights of the taxpayer under IRC § 7431

Destruction of Tax Information

FTI furnished to the user and any paper material generated from it, such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed by burning or shredding.



Slide Notes

FTI furnished to the user and any paper material generated from it, such as copies, photo impressions, computer printouts, notes, and work papers, must be destroyed by burning or shredding. If a method other than burning or shredding is used, that method must make the FTI unreadable or unusable.

The following guidelines must be observed when destroying paper FTI:

Burning: The material must be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated.

Shredding: Destroy paper using crosscut shredders that produce particles that are 1mm x 5mm in size (or smaller) or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 or (2.4mm) security screen.

NOTE: If shredding deviates from the above specifications, FTI must be safeguarded until it reaches the stage where it is rendered unreadable through additional means, such as burning or pulping.

Slide Notes, cont.

Hand tearing, recycling, or burying information in a landfill are unacceptable methods of disposal.

FTI furnished or stored in electronic format must be destroyed in the following manner: Electronic media such as (hard drives, tapes, CDs, and flash media) must be destroyed according to guidance in NIST Control MP-6, Media Sanitization, and Section 2.F.3.1, Media Sanitization.

Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subjected to electromagnetic erasing. If reuse is not intended, the tape must be destroyed by burning or shredding in accordance with applicable standards.

Destroy microfilms (microfilm, microfiche, or other reduced image photo negatives) by burning.

When in doubt about how to dispose of tax information, please contact the Chief Information Security Officer.

Payment Card Industry

DOR must adhere to PCI requirements. In the event your job or role requires a business need for you to collect credit card data from a taxpayer, certain precautions must be used in regard to handling and protecting this data.



If you need to dispose of the card information in printed format, remember that the cardholder data must be disposed of in such a way that it cannot be reconstructed.

Slide Notes

DOR must adhere to PCI requirements. In the event your job or role requires a business need for you to collect credit card data from a taxpayer, certain precautions must be used in regard to handling and protecting this data.

- DOR staff must never store the CVC, or Card Verification Code.
- Never request the card verification code from the taxpayer.
- Never store the card verification code which is sometimes called the PIN verification code. This includes writing the code on paper. NOTE: This is the 3- or 4-digit code found on the back of credit cards or on the front of cards like American Express.
- The payment card industry allows us to store the 16-digit primary account number, which is located on the front or back of the card, but it must be stored in an encrypted format. Revenue stores this number encrypted and this is handled by our IT Department.

If you need to dispose of the card information in printed format, remember that the cardholder data must be disposed of in a way that it cannot be reconstructed.

What is PII?

Personal Identifiable Information, or PII, includes a person's name, or their first initial plus last name, in combination with various types of identification numbers.

Data classified as **confidential** must be properly handled and protected accordingly (North Carolina General Statute 75-66).

Person Definition

Person definition under NC PII laws, as defined in North Carolina General Statute 75-61(9), is any individual, partnership, corporation, trust, estate, cooperative, association, government subdivision or agency, or other entity.



Types of PII

It's important for employees to understand what types of information are considered PII.



Slide Notes

It's important for employees to understand what types of information are considered to be PII. Personal Identifiable Information may include, under North Carolina General Statute 14-113.20:

- Social security or employer taxpayer identification numbers
- Driver's license
- State identification card or passport numbers
- Checking account numbers
- Saving account numbers
- Credit card numbers
- Debit card numbers




Types of PII, cont.



Slide Notes

- Personal Identification Code, or PIN, as defined in General Statute 14-113.8(6)
- Electronic identification numbers, electronic mail names, or addresses
- Internet account numbers or Internet identification names
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage

All Possible

-  Occasionally, you may run across data that is classified as All Possible.
-  This is the highest classification we have at the DOR.
-  All the regulations and requirements that apply to FTI, Confidential, or Public Data would apply to this type of data.

Key Points to Remember



- 01** **Data Classifications:** There are four data classifications used at Revenue (Federal Tax Information, Confidential Information, Public Information, and All Possible). All Possible, Federal Tax Information, and Confidential Information should be handled with care.
- 02** **Federal Tax Information (FTI)** is categorized as Sensitive but Unclassified information or (SBU) and may contain personally identifiable information (PII). FTI is taxpayer information received directly from the IRS and may include the taxpayer's name, social security number, or their address.
- 03** **Commingled Data:** Commingling of FTI refers to having FTI and non-FTI data stored together, regardless of format. Federal taxpayer information combined with state tax information is referred to as commingled data.
- 04** **PII Examples:** It is important for employees to understand what types of information are considered personal identifiable information (PII). Examples of PII could include an individual's first, last name, their social security number, or a business name, and a tax identification number.
- 05** **Return Information** is any information collected or generated by the IRS regarding any person's liability or possible liability under the Internal Revenue Code (IRC). Confidentiality and disclosure of returns and return information describes Internal Revenue Code IRC 6103.
- 06** **Public Records** may include documents, paper, email, text messages, or other means used to transact state business by any agency of North Carolina government and are the property of the people as defined in North Carolina General Statute 132-1.

Thank You!

You are our first line of defense when it comes to cyber threats!

If you have questions regarding the information covered in this eModule or if you suspect a security incident has occurred, report it to the DOR IT Service Desk at (919) 754-2323 or email the Service Desk at ServiceDesk@ncdor.gov.

Acknowledgements



eLearning Course Developer
Evette Tillery
Sr. Instructional Designer
Talent Management



Voice Over
Thomas Beam
Information & Communications Spec. III
Public Information Office



Resources and Images
Articulate Storyline Content
Library 360 Assets, iStock
Photos, and Unsplash.com



Slide Notes

This concludes the section on State and Federal tax Information and Regulations.

You are our first line of defense when it comes to cyber threats!

If you have questions regarding the information covered in this eModule or if you suspect a security incident has occurred, report it to the DOR IT Service Desk at (919) 754-2323 or email the Service Desk at ServiceDesk@ncdor.gov.

SECTION 2: Staff Security Responsibilities and Facility Security Reminders



Slide Notes

Welcome to the Staff Security Responsibilities and Facility Security Reminders, where you will learn more about the role you play in helping to protect your agency.

The first section covers topics such as Email, Social Media, Mobile Resources, Best Practices for preventing System Viruses, eMedia, the DOR Shared Drive, and Password Best Practices.

The last section discusses facility security reminders and includes information on alternative worksites, facility safeguards, and situational awareness.

Learning Objectives



Describe staff security responsibilities



Discuss facility security reminders

Slide Notes

At the conclusion of this eModule, you'll be able to:

- Describe staff security responsibilities
- Discuss facility security reminders

Staff Security Responsibilities



No Federal Tax Information or confidential information shall be transmitted over the Internet without prior approval of the Chief Information Security Officer.

Slide Notes

Although agency staff members have access to the Internet, please remember the following safety precautions:

- Internet usage is monitored for all staff members.
- Do not download any software without prior approval from the Chief Information Security Officer.
- Elevated privileges that require internet or email access must be approved by the Chief Information Security Officer.
- Any approved files downloaded from the Internet must be scanned for viruses.
- No Federal Tax Information or Confidential information shall be transmitted over the Internet without prior approval of the Chief Information Security Officer. This is to ensure the communication is approved and is sent using approved secure methods.

NCDOR Email Account

- Email sent through your NCDOR email account is considered public record.
- Before hitting send, ensure that the information you are sending is something you would be comfortable with the public having access to.



NCDOR Email Account and Fax

When using a messaging system, such as email or fax, please remember, confidential and FTI should only be disclosed to authorized recipients.

- Follow all guidelines and protocols
- Provide adequate labeling and protection
- Include a cover sheet on fax transmissions
- A notification of the sensitivity of the data and need for protection
- A notice to unintended recipients via telephone to report the disclosure and confirm destruction



Slide Notes

When using a messaging system, such as email or fax please remember, confidential information and FTI should only be disclosed to authorized recipients with an established business need, and the information must be used for processing a valid business request.

Staff must:

- Follow all guidelines and protocols related to sending Agency Data internally and/or externally
- Provide the adequate labeling (e.g., email subject contains FTI) and protection
- Include a cover sheet on fax transmissions that explicitly provides guidance to the recipient, that includes:
- A notification of the sensitivity of the data and the need for protection
- A notice to unintended recipients via telephone to report the disclosure and confirm destruction of the information.

NCDOR employees must immediately report any email or fax containing Agency Data, such as FTI that is inadvertently sent to the wrong person or that is in violation of the Agency's Policy to the DOR IT Service Desk at ServiceDesk@ncdor.gov or (919) 754-2323.

Prohibited Uses of Email and Fax

Prohibited uses of email include, but are not limited to:

1

Distribution of insulting, offensive, or disruptive messages

2

Opening email attachments from unknown sources

3

Use of third-party email sources to send communications

4

Represent personal opinions not authorized by the agency

5

Sharing email passwords or account passwords

6

Solicitation or persuasion of commercial ventures

7

Send (upload) or receive (download) copyrighted materials

8

Solicit non-agency business for personal gain or profit

Slide Notes

Prohibited uses of e-mail include, but are not limited to:

- The distribution of insulting, offensive, or disruptive messages. Among those which are considered offensive, are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.
- Opening e-mail attachments from unknown or unsigned sources.
- Use of third-party email sources to send communications on behalf of the Agency.
- Represent personal opinions not authorized by the Agency.
- Sharing email passwords account passwords.
- The solicitation or persuasion of commercial ventures, religious or political causes, outside organizations, or to other non-job-related solicitations
- To send (upload) or receive (download) copyrighted materials, proprietary company information, or similar materials without prior authorization.
- Solicit non-agency business for personal profit or gain.

The slide features five blue rectangular boxes with white text, arranged in two rows. The top row contains three boxes, and the bottom row contains two boxes. Each box contains a number followed by a security rule.

- 9** Send agency data without using approved method of encryption
- 10** Excessive personal use of company email resources is prohibited
- 11** Do not transmit agency data to or from a non-agency email address.
- 12** Never use email while logged into an administrator account.
- 13** All messages will be archived and subject to NC Public Records law.

Slide Notes, cont.

- Send Agency Data without using an approved method of encryption.
- Excessive personal use of company email Resources is prohibited.
- No Agency Data shall be transmitted to or from a non-Agency email address without prior approval of the CISO.
- Email must never be used while logged into an administrator account. A non-administrator account must be used instead.
- All messages will be archived and will be subject to North Carolina Public Records law. N.C.G.S. §132 defines public records as “documents, papers, letters, regardless of physical form or characteristics, made or received in connection with the transaction of public business.” Email, text messages, and messages related to public business may be disclosed to third parties.

DOR Staff/Contractor with Virtual Desktop Infrastructure (VDI)



The agency allows connections from external information systems only in the event that the agency has configured a virtual desktop infrastructure (VDI) solution.



Approval by the agency CISO is required for connection of non-governmental-furnished or contractor-owned IT devices.

Slide Notes

The Agency allows connections from external information systems only in the event the Agency has configured a virtual desktop infrastructure (VDI) solution to receive, secure and manage remote connections.

Approval by the Agency CISO is required for connection of non-government furnished or contractor-owned IT devices (including USB-connected portable storage and mobile devices) to agency resources receiving, processing, storing, accessing, protecting and/or transmitting Agency Data. This requirement does not apply to networks and systems intended for use by the public.

Staff must not:

- Use messaging systems for harassment, discrimination, to distribute objectionable or illicit material, disrupt work, transmit large files, or in a manner that violates local, state, or federal laws.
- Take photographs, use image capture tools, or other mechanisms to capture images or data from DOR systems when accessing the VDI environment from a device not provided by the DOR.
- Have cameras capture Confidential or FTI information within the video stream.

Social Media

Posting to social media regarding an incident is considered indirectly communicating with the media.

The Public Affairs office is designated as the only department:

- authorized to communicate with the media
- to make statements on behalf of the agency on social media regarding incidents on any other issue

Social Media

There are many social media outlets and all are easily accessible.

- **Do not make** a statement about the Department of Revenue using these outlets.
- **Do not make** statements about Revenue on social media or use Revenue logos, letterhead, etc.
- **Do not make** offensive comments or engage in communications that violate the privacy or public rights of others

Lock Your Computer



Protect the access of information by locking your computer. Before you leave your seat, always lock or shut down your computer when unattended.

Lock your screen by using the following key combinations:

- **Ctrl + Alt + Delete, then select Lock**
- **Press the Windows key + L key**

Slide Notes

Along with creating and using strong passwords, you can also protect the access of information by locking your computer. Because you are responsible for any activity that takes place under your User ID, it is required that before you leave your seat, always lock, or shut down your computer when unattended.

You can lock your screen by using the following key combinations:

Ctrl + Alt + Delete, then select Lock

Or

Press the Windows key + L key

By taking these appropriate measures, it will help to safeguard not only yourself but also taxpayer information.

Mobile Resources inside DOR

You are responsible for the security of any mobile resources assigned to you!

Inside DOR Facilities – Mobile resources are considered secure unless otherwise indicated.

Contact the Service Desk immediately in the event of a device being lost or stolen.

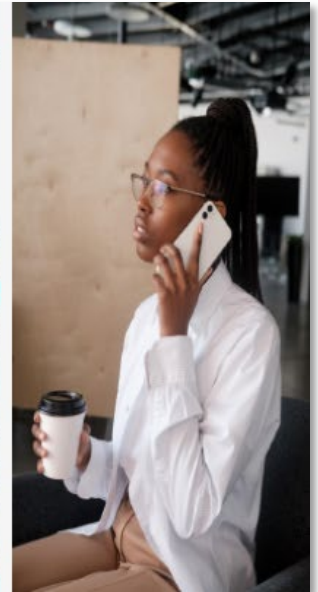


Mobile Resources outside DOR

Outside of DOR – Mobile resources should be stored out of plain sight and when possible under lock and key.

When traveling by common carrier, mobile resources should not be checked as baggage.

Remember to contact the Service Desk immediately in the event of a device being lost or stolen.



eMedia Best Practices



Do not install or connect any non-DOR issued hardware or media to any DOR device or the DOR network.

The only exception is if there is a valid business need and proper precautions have been taken.

If there is a valid business need to receive external electronic removable media, or eMedia from a taxpayer, always disconnect from the DOR network and scan the eMedia for malicious content before it can be stored or used on any DOR resource.

The Scanning Files for Threats Using Cortex XDR Desk Instructions located in ServiceNow should be followed for scanning eMedia. Refer to Knowledge Base Article # KB0012042. The Knowledge Base article is also included as a PDF attachment in the learning plan.

DOR Shared Drive Best Practices



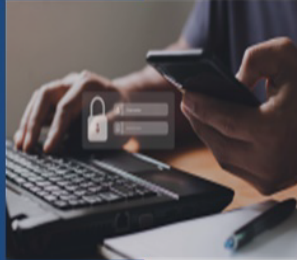
Approved solutions other than the H Shared drive should be used whenever possible to share confidential data.

Confidential data saved on the H Shared drive should be removed by the receiving party as soon as possible.

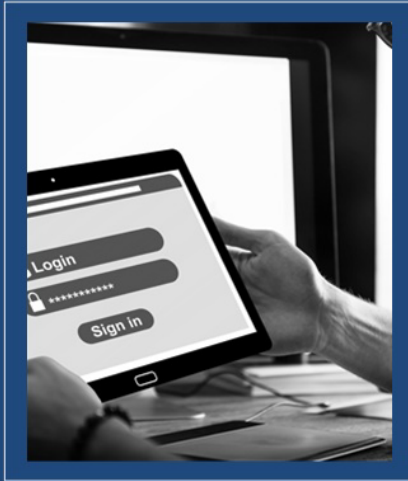
- The H Shared drive should only be used for temporary storage of all data including confidential data.
- The employee sharing data should ensure the person with whom they are sharing data is authorized.

Password Best Practices

For the safety and security of the data housed at Revenue, our systems require passwords, and in some cases, multiple passwords, to access information.



- To improve the security of system passwords, they should be complex and contain at least eight characters utilizing a combination of upper and lower case letters, numbers, and special characters.
- Remember, the complexity of your password is nice, but the length of your password is key.



Password Best Practices, cont.

Here are some password best practices in regard to password safety:

Revenue staff should not:

- share passwords with other staff members
- store passwords in any electronic communication
- embed passwords in automated programs, utilities, or applications
- use words included in a dictionary or popular phrases

System intruders may try to use special tools called "password crackers" that include all dictionary words.

Creating Secure Passwords

Weak passwords are quite common.

- The image on the right displays the 10 weakest passwords used in 2023.
- These passwords are prime examples of passwords that can be easily cracked using hacking tools.

123456	Qwerty123
123456789	1q2w3e
Qwerty	12345678
Password	111111
12345	1234567890

Source: <https://securityboulevard.com/2023/05/worlds-worst-passwords-is-it-time-to-change-yours/>

Creating a Passphrase

A **passphrase** is one of the most secure types of passwords and is the recommended method to use when creating a password.

- A passphrase is easy for you to remember but hard for others to guess.
- You can add to the complexity by substituting some of the letters for symbols and numbers.

Passphrase Hint	Passphrase
I would like my password to be very secure!	lwImp2bvs!
Why does it take so long to come up with a new password?	Wditsltcuw@np?
The month of October is Security Awareness month!	Tmo0iSAm!

In the three examples provided, notice that some words or letters were substituted for numbers, symbols, and capital letters.

Alternative Work sites



Alternative work sites are places where staff need to access Revenue information while away from a Revenue facility.

- Staff should refrain from accessing or discussing Revenue business in public areas (e.g., airports or coffee shops).
- Discussing Revenue information in public areas may put staff at risk of making an unauthorized disclosure of confidential information.

Alternative Work sites, cont.

There may be situations where staff need to use or access Revenue information while away from a Revenue facility.



Customer's
Tax Office



Employee's
Hotel Room



Teleworker's
Home Office

Remember to refrain from accessing or discussing Revenue business in public areas!

Slide Notes

There may be situations where staff need to use or access Revenue information while away from Revenue facility. These locations are considered alternative work sites.

Some examples of acceptable alternative work sites may include:

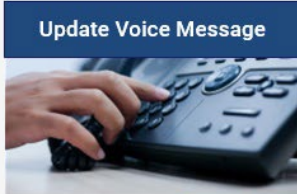
- A customer's tax office
- An employee's hotel room during official business travel
- A teleworker's home office

Even though staff may be conducting official business with a customer, staff are reminded to refrain from accessing or discussing Revenue business in public areas, such as airports or coffee shops.

Discussing Revenue information in these types of locations may put staff at risk of making an unauthorized disclosure of confidential information.

Facility Safeguards

The same security safeguards are required when handling confidential information at alternative work sites as when working within a Revenue facility.



Slide Notes

It should also be remembered that the same security safeguards are required when handling confidential information at alternative work sites as when working within a Revenue facility.

Some examples include:

- Update your voice message to inform taxpayers not to leave personal identifiable information (PII, FTI, or STI)
- Forward business calls to your Revenue issued cellular phone that requires a PIN to retrieve messages
- Be aware of your conversation level as not to be overheard by others
- Adhere to the agency's clean desk policy. Put away documents.
- Do not leave documents on your desk when not present, and do not leave confidential information on any unattended computers

Situational Awareness Reminders

- Interruptions and distractions could result in consequences
- Forwarding an email to the wrong person or sending taxpayer information to the wrong taxpayer
- Visible screens and uncovered paperwork have the potential to be seen by individuals who are not authorized



Slide Notes

Here are a few reminders about situational awareness:

- Interruptions and distractions could result in consequences such as sending information to the wrong person.
- For example, forwarding an email to the wrong person or sending taxpayer information to the wrong taxpayer.
- Visible screens and uncovered paperwork have the potential to be seen by individuals who are not authorized.

Key Points to Remember



- 01** **Public Records:** Emails sent through an NCDOR email account are considered public record. Before hitting send, ensure that the information you are sending is something you would be comfortable with the public having access to.
- 02** **Lock Your Computer:** Protect the access of information by locking your computer. Because you are responsible for any activity that takes place under your User ID, always lock your computer screen before leaving your seat or shut down your computer when it is unattended.
- 03** **Software Downloads:** A safety precaution that agency staff should always follow is to **never download** any software without prior approval from the Chief Information Security Officer.
- 04** **PII:** It is important for employees to understand what types of information are considered personal identifiable information (PII). Examples of PII could include an individual's first, last name, their social security number, or a business name, and a tax identification number.
- 05** **Passphrase:** is one of the most secure types of passwords and is the recommended method to use when creating a password. A passphrase is a collection of words that form a phrase or sentence.

Thank You!

You are our first line of defense when it comes to cyber threats!

If you have questions regarding the information covered in this eModule or if you suspect a security incident has occurred, report it to the DOR IT Service Desk at (919) 754-2323 or email the Service Desk at ServiceDesk@ncdor.gov.

Acknowledgements



eLearning Course Developer
Evette Tillery
Sr. Instructional Designer
Talent Management



Voice Over
Christopher Batista
Print Shop Manager
Business Operations



Resources and Images
Articulate Storyline Content
Library 360 Assets, iStock
Photos, and Unsplash.com



Slide Notes

This concludes the section on Staff Security Responsibilities and Facility Security Reminders.

You are our first line of defense when it comes to cyber threats!

If you have questions regarding the information covered in this training, or if you suspect a security incident, report it to the DOR IT Service Desk at (919) 754-2323 or email the Service Desk at ServiceDesk@ncdor.gov.