EFFECTIVE DATE

(03-08-2023)

PURPOSE

(1) This transmits revised IRM 10.5.5, Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements.

MATERIAL CHANGES

(1) IRM 10.5.5.1, Program Scope and Objectives - Subsections added under Program Scope and Objectives applicable to this program include clarified purpose to include attempted unauthorized access or inspection of taxpayer records and updated reference IRM. Added Primary Stakeholders. Updated information on the subsections below:

a. IRM 10.5.5.1.1, Background - Rewrote summary of the Taxpayer Browsing Protection Act and changed the audience to all business units.
b. IRM 10.5.5.1.3, UNAX Program Office Roles – Added Contracting Officer's Responsibilities (COR).
c. IRM 10.5.5.1.4, added Program Management and Review.
d. IRM 10.5.5.1.5, added Program Controls.
e. IRM 10.5.5.1.6, Terms and Acronyms – Changed title, added acronyms to this section and deleted previously separate Acronyms section, and added two terms and definitions for Employee and Inspection. Added Taxpayer First Act (TFA) and updated UNAX definition.
f. IRM 10.5.5.1.7, Related Resources – Added Document 11500, IRS Manager's Guide to Penalty Determinations.

(2) IRM 10.5.5.3, Added clarifications to Servicewide roles and responsibilities for administering the IRS UNAX Program Office including TIGTA partnership information.

(3) IRM 10.5.5.3.2 - Added (7) Managers must ensure that employees who do not have access to Integrated Talent Management (ITM) complete and submit Form 11370, Certification of Annual UNAX Awareness Briefing, after manual completion of the UNAX Briefing.

- Managers of IRS employees are required to sign Form 11370 and submit it to their UNAX Point of Contact for processing
- Managers of contractors are required to sign Form 11370 and submit it to their Contracting Officer's Representative (COR).

(4) IRM 10.5.5.3.3, Added a sentence requiring the Head of Office Designee (HOD) to send back unsigned forms.

(5) IRM 10.5.5.3.4, Contracting Officer's Representative (COR) UNAX Responsibilities, new section added with a sentence requiring CORs to collect and retain Form 11370 and input in ITM if completed manually.

(6) IRM 10.5.5.3.5, Added TIGTA and the UNAX mailbox as options for consulting and asking questions.

(7) IRM 10.5.5.5, Clarified celebrities' definition and added workplace relationships

(8) IRM 10.5.5.6 - Added (6) IRS, through the Incident Management Office, is required to notify

taxpayers whose personal information was intentionally accessed or disclosed without authorization resulting in an administrative proposal of disciplinary or adverse action against an employee. See *IRM 10.5.4.4.6*

(9) Made other editorial clarifications throughout.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.5.5 dated July 10, 2018.

AUDIENCE

All IRS employees and IRS contractors who have staff-like access (including subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers who have staff-like access.

Celia Doggette, Director,
Identity and Records Protection

10.5.5
IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements

Table of Contents

10.5.5.1
(03-08-2023)
Program Scope and Objectives

(1) Purpose: This IRM section details the policies, procedures and requirements regarding unauthorized access, attempted access, or inspection of taxpayer records (UNAX) . Policy Statement 1-1 provides that taxpayers "have the right to expect that the Service will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities." See IRM 1.2.1.2.1(9).

(2) Audience: All business units

(3) Policy and Program Owner: The Identity and Records Protection (IRP) office under Privacy, Governmental Liaison and Disclosure (PGLD) is responsible for administering Servicewide policy, training, and communication provided by the UNAX Program Office.

(4) Primary Stakeholders: All IRS employees and all business units must follow this policy. HCO, PGLD, Cybersecurity, and TIGTA have a role and responsibility in the UNAX program.

10.5.5.1.1
(03-08-2023)
Background

(1) Since the inception of the Integrated Data Retrieval System (IDRS) in 1972, IRS has worked continuously to prevent and detect unauthorized access, attempted access and inspection of taxpayer records (UNAX) in all IRS internal and external computer systems.

(2) After UNAX concerns were reported in 1993, the Service implemented an information system to perform detection analyses of audit trail information.

(3) On August 5, 1997, the Taxpayer Browsing Protection Act (Public Law No. 105-35) (codified at 26 U.S.C. (IRC) 7213A, 7431) was signed into law, making willful unauthorized access or inspection of taxpayer records a crime. "Upon conviction, penalties can include fines up to $1,000 and/or up to one year in prison (together with the costs of prosecution), as well as termination of employment for federal employees. This law also established the right of taxpayers to seek civil damages in federal court."

10.5.5.1.2
(07-10-2018)
Authorities

(1) *Taxpayer Browsing Protection Act (Public Law No. 105-35).*

(2) IRC 7213A, Unauthorized inspection of returns or return information.

(3) IRC 7431, Civil Damages for Unauthorized Inspection or disclosure of returns and return information.

10.5.5.1.3
(03-08-2023)
UNAX Responsibilities

(1) IRM 10.5.5.3 through IRM 10.5.5.3.4 contain UNAX roles and responsibilities for:

a. Servicewide applications
b. The IRP office
c. IRS managers
d. Head of Office Designee (HOD)
e. Contractors and Contracting Officer's Representative (COR)
f. IRS employees

10.5.5.1.4
(03-08-2023)
Program Management and Review

(1) IRP in PGLD manages the UNAX Program through the following reviews and reports:

a. Annual Review of UNAX Awareness Briefing – formal review of mandatory briefing which includes updates when needed, and development of new UNAX vignettes periodically to keep employees engaged and mitigate potential UNAX violations.
b. ALERTS Statistics and Metrics – Retrieve extract from Automated Labor and Employee Relations Tracking System (ALERTS) and analyze extract to assess Servicewide statistics and metrics for unauthorized access including the number of employees that were removed, resigned, prosecuted, suspended, cleared, or had other administrative actions taken.

10.5.5.1.5
(03-08-2023)
Program Controls

(1) UNAX Certification – The Service requires employees to complete the Annual UNAX Mandatory Awareness briefing and certify they completed the briefing regardless of whether they have access to taxpayer information. Every employee is responsible for protecting the confidentiality and privacy of taxpayer information.

(2) Annual UNAX Completion Report – review information from HCO regarding completion rate for mandatory briefing cycle and share July – October completion reports with business units points of contacts.

10.5.5.1.6
(03-08-2023)
Terms and Acronyms

(1) **UNAX:** The willful unauthorized access, attempted access or inspection of taxpayer returns or return information.

(2) **Employee**: Includes all IRS personnel. Also includes all contractors who have staff-like access. .

(3) **Staff-like access**: This is when a contracted individual is granted access to IRS facilities or IRS systems, or has opportunity to be exposed to IRS information.

(4) **Covered Relationships**: Personal or outside business relationships that can raise questions about the employee's impartiality in the handling of a tax matter.

(5) **Inspection:** The terms "inspected" and "inspection" mean any observation, review, or examination of a return or return information (paper or electronic).

(6) The following table contains definitions for the acronyms most commonly used in this IRM:

Acronym	Definition
AMS	Accounts Management System
COR	Contracting Officer's Representative
EUP	Employee User Portal
HCO	Human Capital Office
HOD	Head of Office Designee
IDRS	Integrated Data Retrieval System

Acronym	Definition
IRC	Internal Revenue Code
IRP	Identity and Records Protection
ISA	Inadvertent Sensitive Access
IT	Information Technology
PGLD	Privacy, Governmental Liaison and Disclosure
MOR	Manager of Record
RUP	Registered User Portal
TFA	Taxpayer First Act
TIGTA	Treasury Inspector General for Tax Administration
TDS	Transcript Delivery System
UNAX	Unauthorized access or inspection of taxpayer records (or attempts)

10.5.5.1.7
(03-08-2023)
Related Resources

(1) UNAX Knowledge Base site at: *https://portal.ds.irsnet.gov/sites/vl003/lists/unax1/landingview.aspx*.

(2) Document 10281, Safeguarding Taxpayer Records Renewing Our Commitment - UNAX Employee Booklet.

(3) Document 12612, Stop UNAX In Its Tracks.

(4) Document 12692, UNAX If/Then Chart.

(5) Document 11500, IRS Manager's Guide to Penalty Determinations.

10.5.5.2
(07-10-2018)
IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program

(1) To implement the requirements of the Taxpayer Browsing Protection Act (Public Law No. 105-35), the IRS created the willful unauthorized access, attempted access or inspection of taxpayer records (UNAX) Program Office. The Taxpayer Browsing Protection Act, in conjunction with the UNAX program, provides the following:

a. Willful unauthorized access or inspection of taxpayer records is a crime, punishable upon conviction, by fines, imprisonment, and termination of employment. Taxpayer records include hard copies of returns and return information, as well as returns and return information maintained on a computer.
b. When IRS employees are criminally charged, the IRS is required to notify taxpayers as soon as practicable that their records have been accessed without authorization and of their right to seek civil action for damages.
c. A taxpayer who is a victim of unlawful access or inspection has the right to take legal action even if the taxpayer's information is never revealed to a third party.

d. For contractors, the willful unauthorized access or inspection of taxpayer records can result in removal from the contract. Furthermore, upon conviction, it can result in fines, and/or imprisonment of not more than one year, together with the costs of prosecution.
e. Criminal UNAX violations result from willful unauthorized inspection of returns and return information. Under 26 USC IRC 7213A, the violation is punishable by a fine not to exceed $1,000 or imprisonment of not more than 1 year, or both, together with the costs of prosecution. Upon conviction, the employee is terminated.
f. UNAX violations may also result in penalties for misuse of a government computer.
g. Non-Criminal Penalties – pursuant to IRS UNAX policy, removal is to be proposed for all UNAX violations. The penalty can be mitigated by the deciding official at the decision stage.
h. Using information gained from a UNAX violation can lead to additional criminal charges such as falsification of records, fraud, embezzlement and identity theft.
i. This willful unauthorized disclosure of tax return or return information is a felony.

(2) IRS UNAX policy provides that employees may be subject to administrative penalties for the willful and unauthorized attempted access of their own or another taxpayer's records.

a. Administrative penalties include but are not limited to:

• Removal of employee

• Suspension of employee

b. Additional information on penalties for UNAX violations can be found in Document 11500, IRS Manager's Guide to Penalty Determinations.

(3) The IRS relies on the ethics and integrity of its employees and enlists their support in eliminating cases of UNAX. Employees who have knowledge of a suspected UNAX violation, must report it to TIGTA, or their managers.

10.5.5.3
(03-08-2023)
Servicewide Roles and Responsibilities for Administering the IRS UNAX Program

(1) Human Capital Office (HCO) Labor/Employee Relations & Negotiations (LERN) is responsible for managing the administrative adjudication of confirmed UNAX cases. This office coordinates with TIGTA and the Office of Chief Counsel, General Legal Services (GLS) to ensure employees are treated fairly and equitably in every UNAX case. LERN is responsible for:

a. Tracking and reporting UNAX case status from inception to final disposition.
b. Preparing the necessary documents in support of the administrative actions taken by management.
c. Forwarding the necessary documents to management.
d. Providing consultative support to management for administration of appropriate discipline.
e. Notifying management of their responsibility to remove employees from systems when a UNAX case is received or when management becomes aware of a potential UNAX violation.

(2) Information Technology (IT) Cybersecurity is responsible for reviewing and certifying various data security reports. Cybersecurity performs system tasks of

detecting, reporting, escalating, and referring behavioral anomalies indicating potential UNAX violations to IRS stakeholders. Cybersecurity must analyze and partner with management to determine the validity of account-related accesses. Questionable accesses are referred to TIGTA for investigationas potential UNAX violations.

Note: See IRM 10.8.1.3.3 for more information on Audit & Accountability Policy and Procedures.

(3) The IRS organizations assign business unit Points of Contact (POCs) for the Annual UNAX Awareness Briefing and Certification. They are responsible for the following:

a. Attending meetings to discuss data security – including UNAX.
b. Working with PGLD UNAX Program Office and their business unit managers to ensure all their business unit employees complete the required briefings and certifications.
c. Supporting the Annual UNAX Briefing process by collecting and accounting for Form 11370, Certification of UNAX Annual Awareness Briefing for employees in their business units unable to complete the briefing online.
d. Submitting completed Forms 11370 to National Archives and Records Administration (NARA) at opf.con.site@irs.gov for inclusion in employee's Official Personnel Folder.
e. Reviewing the business unit's completion statistics.
f. Informing management officials of the business unit's UNAX Awareness Briefing completion rates.

(4) Facilities Management and Security Services (FMSS) ensures system and facility accesses are removed when an employee separates. .

(5) TIGTA is responsible for investigating all potential UNAX allegations received and notifying appropriate management officials that a UNAX investigation has been initiated. This responsibility includes but is not limited to potential computer inspection techniques and computer system generated audit trails. Substantiated UNAX violations will be referred to the Department of Justice for criminal prosecution. TIGTA partners with the UNAX Program Office for quarterly partnership meetings to provide updates and status on action items. TIGTA participates annually with the UNAX Program Office when conducting UNAX Live/Virtual Forums to expand awareness of UNAX policies and educate employees about preventing UNAX violations.

(6) The UNAX Program Office, within PGLD, develops and distributes UNAX educational materials, including the Annual UNAX Awareness Briefing aimed at preventing and reducing the number of UNAX incidents.

(7) The Incident Management Office, within PGLD, is required to notify taxpayers whose personal information was intentionally accessed or disclosed without authorization resulting in an administrative proposal of disciplinary or adverse action against an employee. See *IRM 10.5.4.4.6*

(8) All Senior Executives and managers (including CORs and MORs) are responsible for:

a. Monitoring, assigning or removing employee access to IRS computing systems as needed based on assigned IRS duties. Systems that must be monitored include (but are not limited to): Integrated Data Retrieval System (IDRS), Modernized e-File (MeF), Accounts Management System (AMS), Transcript Delivery System (TDS), Registered User Portal (RUP), Employee User Portal (EUP), Information Return Intake System (IRIS)etc.
b. Approving employee access to any internal or external IRS computer system only when required to complete official IRS duties as assigned by management.
c. Removing access to any internal or external computer system when it is no longer required to complete official IRS duties as assigned by management.
d. Discussing necessary actions and possible discipline with servicing LR Specialist once notified of the investigation.

(9) All IRS employees are responsible for:

a. Accessing IRS paper or electronic tax records or tax information only when it is required to complete official IRS duties as assigned by management.
b. Informing their managers when they no longer require access to a specific IRS internal or external computer system or command code requiring administrative approval.
c. Refraining from unauthorized access of tax information.
d. Refraining from accessing their own records, or records of anyone with whom they have a covered relationship. See IRM 10.5.5.5, Covered Relationships.
e. Refraining from accessing information unless the access is required by their duties as assigned by management.
f. Completing PGLD mandatory briefings, which include UNAX, PIPD, RM.

10.5.5.3.1
(03-08-2023)
UNAX Program Office Roles and Responsibilities

(1) The IRS is committed to preventing the willful unauthorized access, attempted access, and inspection of taxpayer records (UNAX). The UNAX Program Office's mission is to ensure all employees:

a. Understand what UNAX is.
b. Understand what the consequences of accessing, attempting to access, or inspecting taxpayer records or tax information (electronic or paper) for other than management authorized tax administration reasons.
c. Work to prevent all instances of UNAX violations. Please refer to the UNAX Knowledge Management site for additional information:*https://portal.ds.irsnet.gov/sites/vl003/Lists/UNAX1/DispItemForm.aspx?ID=1*

(2) The UNAX Program Office must develop and implement a Servicewide UNAX Program in partnership with TIGTA, HCO, IT Cybersecurity, and other stakeholders that includes:

a. UNAX education
b. UNAX detection through analysis of accesses to IRS systems and unauthorized access complaint investigations
c. UNAX policy compliance .

(3) The UNAX Program Office must, in partnership with TIGTA, HCO, IT Cybersecurity, and other stakeholders take action to:

a. Mitigate weaknesses in programs and systems that lead to low UNAX compliance rates.
b. Identify areas for compliance improvement.
c. zProvide training
d. Implement other measures designed to foster voluntary UNAX compliance to include periodic communications, outreach ad hoc training and UNAX Forums
e. Reduce willful unauthorized access, attempted access, and inspection of taxpayer records.

(4) The UNAX Program Office must:

a. Update, administer and maintain the IRS UNAX website containing information, policies, procedures, forms and links that support the UNAX Program .
b. Manage the Servicewide Annual UNAX Awareness Briefing Certification Program to include:

Item	Description
I	Review and update, in partnership with all stakeholders, UNAX briefing materials to keep information current, relevant and effective;
ii	Track the numbers of employees who take the annual UNAX mandatory briefing, and provide relevant statistical data to IRS executive leadership;
iii	Request Senior officials to designate UNAX coordinators for their respective organizations on a yearly basis;
iv	Provide instruction and guidance to business unit UNAX points of contact (POCs) prior to and during the annual Servicewide mandatory briefing cycle to ensure accurate reporting of the numbers of employees who complete the briefing;
v	Prepare and deliver reports to senior officials that track the numbers of employees who take the mandatory briefing , and
vi	Contact business unit POCs who have low rates of compliance, requesting their employees complete the UNAX briefing.

c. Notify taxpayer victims when a person is charged criminally by indictment or information with unauthorized inspection as required by IRC 7431(e). Notification letters will be sent to victims to alert the taxpayer of permissible next steps.
d. .
e. Provide all managers the guidance and tools needed to help them maintain an ongoing dialogue with their employees about UNAX violations and the consequences and penalties for willfully accessing, attempting to access, or inspecting taxpayer records for other than authorized tax administrative duties as officially assigned by management.
f. Respond to inquiries from managers, employees and taxpayers concerning UNAX reporting requirements and other UNAX inquiries or refer them to other UNAX subject matter experts and stakeholders as appropriate.

g. Educate Senior officials and managers that all employees returning to work after UNAX disciplinary actions must complete UNAX mandatory briefing and UNAX recertification before they may access any system with taxpayer information.
h. Develop and distribute comprehensive "just-in-time" Servicewide communications for all employees to assist them in understanding the importance of the mandatory Annual UNAX Awareness Briefing and the rules for certifying that the briefing was completed.

10.5.5.3.2 (03-08-2023) **Manager UNAX Responsibilities**

(1) Managers must take an active role to prevent willful and attempted unauthorized access, and inspection of taxpayer information in electronic and paper form. This involves overseeing employees' work as well as continually stressing the importance of protecting and securing taxpayer records.

(2) IRS Manager's Guide to Penalty Determinations (Document 11500) states that managers may be subject to written reprimand, suspension or removal for failure to adequately instruct, train, or supervise employees in their responsibilities for record and information protection.

(3) Managers must communicate with employees on a regular basis to ensure they are aware of UNAX prohibitions and the penalties. Communication also ensures employees know how to document and report inadvertent or unintentional access.

(4) Managers are responsible for the timely and thorough review of available system security reports. Managers must report suspected UNAX violations or any unusual activity to TIGTA for investigation.

(5) Managers must monitor and ensure that employees have access to IRS internal or external computer systems containing taxpayer information only when necessary to complete their IRS officially assigned duties.

(6) Managers must ensure employees who are being investigated for UNAX violations are promptly removed from IDRS and any other IRS computer system requiring administrative approval and containing taxpayer information. Managers must also ensure these employees are removed from other tax related duties.

(7) Managers must ensure that employees who do not have access to Integrated Talent Management (ITM) complete and submit Form 11370, Certification of Annual UNAX Awareness Briefing, after manual completion of the UNAX Briefing.

- Managers of IRS employees are required to sign Form 11370 and submit it to their UNAX Point of Contact for processing.
- Managers of contractors are required to sign Form 11370 and submit it to their Contracting Officer's Representative (COR).

(8) Managers must sign and timely submit Form 11377 or Form 11377-E, Taxpayer Data Access, to the designated head of office designee. Form 11377 or Form 11377-E are used to document accesses to taxpayer information not supported by direct case assignment or which may otherwise appear questionable. A manager's signature on this form does not imply authorization for documented accesses. The access may still be subjected to further review and investigation.

(9) Managers must make fair and timely reassignments whenever an employee reports having a covered relationship with an individual or organization in an assigned tax matter which may create a conflict of interest. Form 4442, Inquiry Referral, may be used by the employee to request such reassignments, thus avoiding a conflict of interest.

(10) Managers must educate employees to avoid UNAX violations, and ensure employees know the consequences of their actions.

(11) Managers must lead by example.

(12) Managers must ensure their employees' access of IRS internal or external computer system is:

a. Controlled through Business Entitlement Access Request System (BEARS) approval process.
b. Granted only when required to complete official duties.
c. Removed when no longer required to complete official duties.

10.5.5.3.3
(03-08-2023)
Head of Office Designee (HOD) UNAX Responsibilities

(1) All HODs are responsible for protecting the confidentiality and privacy of taxpayer information to which they have access.

(2) The HOD receives Form 11377 or Form 11377-E from managers and prepares them for storage.

(3) The HOD must return all unsigned forms to appropriate manager for employee signature.

(4) The HOD is responsible for uploading signed Forms 11377/11377-E into the Taxpayer Data Access Library where they are maintained for six years.

Note: More detailed instructions for these responsibilities are found in the HOD Guide in the Taxpayer Data Access Library.

10.5.5.3.4
(03-08-2023)
Contracting Officer's Representative (COR) UNAX Responsibilities

(1) The Manager of Record (MOR) or Contracting Officer's Representative (COR) is responsible for ensuring contractors with staff-like access meet the mandatory briefing requirements. Upon on-boarding, all contractors with staff-like access must complete PGLD mandatory briefings which include Unauthorized Access (UNAX), Privacy, Information Protection and Disclosure (PIPD), and Records Management (RM) within 5 business days of being granted staff-like access and then repeat the training annually thereafter. For a definition of staff-like access see IRM 10.5.5.1.6(3).

(2) If the contractor does not have access to ITM, CORs must enter the training information into ITM so the contractor receives credit for completing the training. All CORs are responsible for collecting, signing, and retaining Forms 11370, Certification of Annual UNAX Awareness Briefing, received from contractors. Certification forms must be stored in a locked container, security container or a secure room, wherever the location. For more information, please see IRM IRM 10.2.18, Physical Access Control, and *Internal Revenue Service Acquisition Policy 1052*.

10.5.5.3.5
(03-08-2023)
Employee UNAX Responsibilities

(1) All IRS employees (including managers, executives and contractors who have staff-like access) are responsible for protecting the confidentiality and privacy of taxpayer information to which they have access. Employees are responsible for understanding what UNAX means and what the potential consequences are for the willful unauthorized access, attempted access, or inspection of paper or electronic taxpayer records. If they are uncertain whether access or inspection is appropriate, they should first consult with a manager, TIGTA, or send questions via email to *UNAX. Employees are only allowed to access tax return information when it is needed to carry out their assigned tax administrative duties and there is no covered relationship.

(2) Employees are prohibited from browsing or inspecting a celebrity or politician's return or return information without authorization constitutes a UNAX violation with potential for fines, imprisonment, and dismissal. Employees have no legitimate tax-related reason to access the account of a celebrity or politician unless they receive the matter through official channels or in the normal course of business. Celebrities (such as a person who is famous, widely known, or frequently in the media/of media interest, e.g., music industry, sports, entertainment, etc) when the information is not needed to carry out tax related duties.

(3) The IRS relies on the ethics and integrity of its employees and enlists their support in eliminating **"all"** cases of UNAX.

(4) Employees are encouraged to fill out and sign Form 11377 or Form 11377-E by close of business on the day of the inadvertent or questionable access (electronic and paper) and forward the signed copy to their manager to document certain inadvertent or questionable accesses that could include one of the following:

- Accessed electronic or paper tax return information in error (such as accidentally entering an incorrect taxpayer identification number).
- Accessed electronic or paper tax return or tax information of another IRS employee on an assigned case before recognizing the individual as someone known to the employee.
- Accessed electronic or paper tax return or tax information on an assigned case of an individual or organization before recognizing it as belonging to a person or business with whom the employee has a personal or business relationship.
- Researched another taxpayer's information because it was related to an assigned case.
- Received requests from management to access taxpayer information on cases not assigned to the employee.

(5) Employees must:

- Review and apply the guidance within this IRM, the **Employee's Guide to Safeguarding Taxpayer Records - Renewing Our Commitment** Document 10281 and other UNAX directives.
- Take the Annual UNAX Awareness Briefing and complete the certification documentation either online or by filling out Form 11370, Certification of Annual UNAX Awareness Briefing, if the briefing was not completed online.

Note: When employees complete the annual UNAX Awareness Briefing outside of the Integrated Talent Management (ITM) system, they must submit Form 11370 to their managers for signature and processing.

- Timely refer cases to management when the employee's personal or business relationship can raise questions concerning a lack of impartiality in handling a tax matter. (Please see covered relationships in IRM 10.5.5.5 for additional information). Employees should use Form 4442, **Inquiry Referral** for this purpose.
- Inform their managers when approved access to an IRS internal or external computer system is no longer required to complete IRS officially assigned duties.
- Report any suspected UNAX violation to their local TIGTA office or to the TIGTA toll free hotline at: 1-800-366-4484. TIGTA is responsible for investigating all UNAX allegations. IRS employees are protected by law from reprisals when they have reasonable cause to report suspected UNAX violations to TIGTA;. r

(6) Employee must refrain from:

- Accessing returns and return information of other employees known to them **unless** approved in writing by management.
- Accessing or asking other IRS employees to access information of individuals with whom they have a **covered relationship.** See IRM 10.5.5.5, Covered Relationships.
- Accessing tax returns or tax return information in any IRS internal or external computer system (e.g., IDRS, AMS, TDS, RUP, EUP, etc.) unless the access is necessary to complete their official IRS duties as assigned by management.
- Accessing tax returns or tax return information on a personal computer if they are not authorized to access the information on their work computer. For example: An IRS employee had formerly held a position as an accountant prior to becoming employed by IRS. He kept his access to the IRS Registered Users Portal (RUP). The employee then accessed tax return information on the RUP of a former client using his personal computer when performing his IRS official duties. This is an unauthorized access of the taxpayer record and a UNAX violation. IRS employees can only access those accounts assigned to them by IRS management as part of their official IRS tax duties.

10.5.5.4
(07-10-2018)
Official Channels

(1) The IRS policy on access to paper and electronic tax returns and return information states "Employees are only allowed access to tax returns and return information when the information is received through official channels and is needed to carry out official IRS tax duties";

(2) Official Channels include:

a. Cases officially assigned by a manager for official IRS business purposes
b. Taxpayer walk-ins
c. Telephone calls from taxpayers
d. Official correspondence

e. Related case inquiries.

(3) Unofficial Channels include:

a. Requests from individuals at social functions and non-work environments
b. Requests received from close friends, close relatives, close neighbors or co-workers whom you know.

10.5.5.5
(03-08-2023)
Covered Relationships

(1) Covered Relationships are those personal or business relationships that can raise questions about the appearance of a lack of impartiality in the handling of a tax matter. As a result, individuals or businesses can be perceived as receiving expedited or preferential treatment that is unavailable to the general taxpayer public. Requests that are not received through the normal course of business or through official or administrative channels can indicate a covered relationship. Employees are not authorized to access the tax records or tax information of anyone with whom they have a covered relationship:

a. Spouse and ex-spouses
b. Children
c. Parents and grandparents
d. Anyone living in their household
e. Close relatives not included above
f. Friends or neighbors with whom they have close relationships
g. Co-workers, supervisors, or others in the workplace with whom there is a personal relationship
h. An individual or organization for which they or their spouse is an officer, trustee, general partner, agent, attorney, consultant, contractor, employee, or member
i. Any other individual or organization with whom they may have a personal or outside business relationship that could raise questions about their lack of impartiality in handling a tax matter.

10.5.5.6
(03-08-2023)
Violations of IRS UNAX Policy

(1) The willful unauthorized access or inspection of taxpayer information - both electronic and paper - is a crime. Upon conviction, employees can be subject to penalties ranging from job loss to fines and prison terms.

(2) The IRS established the IRS Manager's Guide to Penalty Determinations (Document 11500) to cover UNAX violations that are not criminally prosecuted.

(3) Non-criminal/administrative penalties for violating the UNAX policy range from admonishment to removal from federal service.

a. The agency can still take disciplinary action against employees for violating the agency's UNAX policy even when they are not criminally charged with violating the Taxpayer Browsing Protection Act.
b. Temporary employees and employees in a probationary or trail period may be terminated for UNAX violations.

(4) Criminal penalties assessed upon conviction for violating the Taxpayer Browsing Protection Act Include:

a. A fine in any amount not exceeding $1,000
b. Imprisonment of not more than one year
c. Both the fine and imprisonment
d. Cost of prosecution.

(5) Civil penalties: Taxpayers have the right to take legal action against the IRS when they are victims of unlawful access or inspection even if their information is never revealed to a third party. IRS is required to notify taxpayers that their records have been accessed without authorization when an employee is criminally charged.

(6) IRS, through the Incident Management Office, is required to notify taxpayers whose personal information was intentionally accessed or disclosed without authorization resulting in an administrative proposal of disciplinary or adverse action against an employee. See *IRM 10.5.4.4.6*