



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.27

SEPTEMBER 12, 2024

EFFECTIVE DATE

(09-12-2024)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.27, *Information Technology (IT) Security, Personal Use of Government Furnished Information Technology Equipment and Resources*.

MATERIAL CHANGES

- (1) Applied Interim Guidance Memo IT-10-0323-0004, dated March 24, 2023 “**No TikTok on Government Devices**”, which prohibits the installation and usage of TikTok on IRS IT devices.
- (2) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes all prior versions of IRM 10.8.27. Additionally, this IRM was updated to incorporate Interim Guidance # IT-10-0323-0004. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*; IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities* and IRM 10.8.24, **Information Technology (IT) Security, Cloud Computing Security Policy**.

AUDIENCE

IRM 10.8.27 must be distributed to all personnel responsible for ensuring this transmits revised Internal Revenue Manual (IRM) 10.8.27, **Information Technology (IT) Security, Personal Use of Government Furnished Information Technology Equipment and Resources**. This policy applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal
Chief Information Officer

10.8.27

Personal Use of Government Furnished Information Technology Equipment and Resources

Table of Contents

10.8.27.1 Program Scope and Objectives

10.8.27.1.1 Background

10.8.27.1.2 Authority

10.8.27.1.3 Roles and Responsibilities

10.8.27.1.4 Program Management and Review

10.8.27.1.5 Program Controls

10.8.27.1.6 Terms and Acronyms

10.8.27.1.7 Related Resources

10.8.27.2 Risk Acceptance and Risk-Based Decisions

10.8.27.3 General Policy

Exhibits

10.8.27-1 Prohibited Uses of Government Furnished IT Equipment and Resources

10.8.27-2 Terms and Acronyms

10.8.27-3 Related Resources

10.8.27.1
(09-12-2024)
**Program Scope and
Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the personal use of government furnished information technology equipment and resources for non-government purposes within the IRS.
 - a. This policy is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, and **IRM 10.8.24, Cloud Computing Security Policy**, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS personal use of government furnished IT equipment and resources for non-government purposes.
- (2) **Purpose of the Program:** Develop and publish policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this policy apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer.
- (5) **Program Owner:** Cybersecurity Threat Response and Remediation (an organization within Cybersecurity).
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.27.1.1
(09-12-2024)
Background

- (1) This IRM defines the expanding use of IT resources to a growing group of IRS employees in the workplace, increasingly offering new opportunities to meet the IRS mission objectives, as well as agency values, not the least of which are those directed at providing a positive work-life balance and supportive environment for IRS employees, contractors, vendors, and volunteers. A key component of this positive environment is offering the privilege of limited personal use of government furnished IT equipment and resources. This effort requires organizations and users to exercise extreme due care and caution, with regard to the responsibilities of upholding the public trust, ensuring the privacy and security of data, and protecting systems and infrastructure.
- (2) IRM 10.8.27 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS IT Cybersecurity.

10.8.27.1.2
(09-12-2024)
Authority

- (1) All IRS systems and applications must comply with Executive Orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.
- (2) Treasury Directive (TD) 87-04 (January 27, 2012), defines limited personal use of government furnished IT equipment and resources, and establishes

standards and rules of conduct to allow the Department of the Treasury employees the privilege to use government furnished IT equipment and resources for non-government purposes, when such use involves minimal additional expense to the government and does not overburden any of the Department's IT equipment or resources, based on the following authorities:

- Title 5 - Code of Federal Regulations (CFR) - Part 735, Office of Personnel Management, Employee Responsibilities and Conduct
- Title 5 - CFR Part 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Title 5 - CFR Part 3101, Supplemental Standards of Ethical Conduct for Employees of the Department of the Treasury
- Title 31 - CFR Part 0, Department of the Treasury Employee Rules of Conduct

10.8.27.1.3
(11-03-2023)

Roles and Responsibilities

- (1) IRM 10.8.2, Information Technology (IT) Security, IT Security Roles and Responsibilities, defines IRS-wide roles and responsibilities related to IRS information and information system security, and is the authoritative source for such information.

10.8.27.1.4
(09-12-2024)

Program Management and Review

- (1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.
- (2) It is the policy of the IRS:
 - a. To establish and manage an information security program within all its offices. This policy provides uniform policies and guidance to be used by each office.
 - b. To protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
 - c. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, NARA guidance, other regulatory guidance, and best practice methodologies.
 - d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.27.1.5
(09-12-2024)

Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews the IRM annually to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirements checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.

- (2) Security Policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in the process of being revised.
- (3) This IRM applies to all IRS information and information systems, which store, process, or transmit IRS information or connect to an IRS network or system. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for IRS Personal Use of Government Furnished Information Technology Equipment and Resources to:
 - a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
 - b. Prevent unauthorized access to IRS assets.
 - c. Enable IRS IT computing environments to meet the security requirements of this policy and support the business needs of the organization.
- (5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive.

10.8.27.1.6
(09-12-2024)
Terms and Acronyms

- (1) Refer to Exhibit 10.8.27-2, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.27.1.7
(09-12-2024)
Related Resources

- (1) Refer to Exhibit 10.8.27-3, Related Resources, for a list of related resources and references.

10.8.27.2
(09-12-2024)
**Risk Acceptance and
Risk-Based Decisions**

- (1) Any exception to this policy requires the authorizing official to make a risk-based decision.
- (2) Users must submit RBD requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process documented in the Request for Risk Acceptance and Risk-Based Decision (RBD) Standard Operating Procedures (SOP).

#

- (3) Refer to IRM 10.8.1 for additional guidance on Risk Acceptance.

10.8.27.3
(09-12-2024)
General Policy

- (1) Individuals are permitted to access tools and applications available to the general public on "IRS.gov" and tools and applications available on the "IRS 1040 Central" site <https://www.irs.gov/how-to-file-your-taxes-step-by-step> for IRS employees to look up their own tax information.
- (2) Individuals must have no expectation of privacy while using any government furnished IT equipment and resources at any time, including (but not limited to)

accessing the Internet, proxy avoidance server, or email. Individuals must be aware that their rights to privacy do not change even during limited periods of personal use. To the extent that individuals wish their private activities remain private, they must avoid using government furnished IT equipment and resources such as their computer, the Internet or email. The IRS and its systems must protect certain information, such as tax and Privacy Act records; therefore, any use of government furnished resources is subject to monitoring.

- a. See the IRM 10.8.1, subsection “AC-8 System-Use Notifications” for the current banner text.
- (3) It is the policy of the IRS to:
- a. Permit limited personal use of government furnished IT equipment and resources for non-government purposes, when such use involves minimal additional expense to the government, does not overburden any of the Service’s IT resources, and when access to these IT resources is already authorized for official government business.
 - b. Permit limited personal use to individuals during non-duty time for periods of reasonable duration and frequency of use.
 - c. Grant use that does not adversely affect the performance of official duties, result in the loss of an individual’s productivity, or interfere with the mission or operations of the IRS.
 - d. Ensure that computer systems and networks are not used for downloading illegal, inappropriate, or unauthorized content, and untrusted, unapproved, or malicious software.
 - e. Authorize use that does not violate the Office of Government Ethics (OGE) Standards of Ethical Conduct for Employees of the Executive Branch found at 5 Code of Federal Regulations (CFR) Part 2635, the Supplemental Standards of Ethical Conduct for Employees of the Treasury Department found at 5 CFR Part 3101, Employee Responsibilities and Conduct found at 5 CFR Part 735, and the Department of the Treasury Employee Rules of Conduct found at 31 CFR Part 0.
- (4) The IRS is not required to provide access to IT resources if not already provided for an approved business need. Therefore, this policy does not guarantee Internet or email access to those who do not otherwise have it.
- (5) Personal use must incur only minimal additional expense to the government in areas such as:
- a. Communications infrastructure costs (e.g., telephone charges, telecommunications traffic).
 - b. Use of consumables in limited amounts (e.g., paper, ink, toners).
 - c. General wear-and-tear on equipment.
 - d. Minimal data storage on storage devices.
 - e. Minimal network impacts, keeping email message sizes, including attachments, within IRS specified size guidelines.
- (6) Individuals must be aware of IT security controls which are addressed in the following IRMs:
- IRM 1.10.3, *Office of the Commissioner of Internal Revenue, Standards for Using Email*.
 - IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*

- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
 - IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*
 - IRM 10.8.26, *Information Technology (IT) Security, Wireless and Mobile Device Security Policy*
 - IRM 10.5.1, *Privacy and Information Protection, Privacy Policy* related to IRS privacy concerns in safeguarding agency information
- (7) The social networking service TikTok or any successor application or service of TikTok developed or provided by ByteDance Limited or an entity owned by ByteDance Limited must be removed and is prohibited from being accessed by or installed onto IRS IT devices. (OMB M-23-13)
- a. This applies to devices used to perform work by, on behalf of, or in support of the IRS, to include contractor systems.
 - b. Refer to the OMB M-23-13, *"No TikTok on Government Devices" Implementation Guidance* for exceptions to this guidance.

Note: For this requirement, the term "*Information Technology (IT)*" is as defined in 40 U.S. Code § 11101(6).

This Page Intentionally Left Blank

Exhibit 10.8.27-1 (09-12-2024)**Prohibited Uses of Government Furnished IT Equipment and Resources**

Regardless of work status, individuals must remember that some uses of government furnished IT equipment and resources are absolutely forbidden, even during non-duty time. Some examples of prohibited uses are included, but are not limited to, those listed below:

1. Individuals are prohibited from accessing IRS tools and applications used to complete official IRS assigned duties to look up tax information without an officially assigned IRS business need. These include, but are not limited to: (IRS-defined)
 - AMS - Accounts Management System
 - EUP - Employee User Portal
 - IDRS - Integrated Data Retrieval System
 - TDS - Transcript Delivery System

Note: Accessing these systems without an officially assigned IRS business need would constitute an unauthorized access (UNAX) violation. Refer to the UNAX web site for additional guidance on unauthorized access to tax information.

2. In accordance with IRM 1.10.3 ,*Office of the Commissioner of Internal Revenue, Standards for Using Email* and IRM 11.3.1 , *Disclosure of Official Information, Introduction to Disclosure*, individuals must not send emails containing personally identifiable information (PII)/sensitive but unclassified (SBU) data to taxpayers, their authorized representatives, or other external stakeholders even if requested, because of the risk of improper disclosure or exposure, unless specifically authorized.

Note: An exception to this requirement is when a user is sending their own SBU data (including PII) to or from their personal email accounts. Refer to IRM 10.5.1, for additional guidance pertaining to emailing SBU (including PII) with personal accounts.

3. Individuals must not use government furnished IT equipment or resources, as a staging ground or platform to gain unauthorized access to other systems.
4. Individuals are specifically prohibited from using government furnished IT equipment or resources for commercial purposes, in support of "for-profit" activities and ventures, and other outside employment or business activities (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services). This ban also includes individuals' use of government furnished IT equipment or resources to assist relatives, friends, or other persons in such activities (e.g., individuals must not operate or participate in the operation of a business with the use of IRS computers and Internet (i.e., "IRS.gov") resources).
5. Individuals must not use government furnished IT equipment or resources to access, view, or download personal email.
6. Individuals are specifically prohibited from inappropriate internet usage and participation in any activities that open IRS information or systems to security risks. Viewing or accessing the following types of web sites is also prohibited:
 - Pornographic, sexually explicit, or sexually oriented materials.
 - Personal services web sites, such as buyer/seller, dating services, and other online personal sites.
 - Hacker sites (sites which open the IRS to unacceptable security risk) regardless of the security risks or lack thereof.
 - Materials related to gambling (legal and illegal), terrorist activities, illegal weapons, and any other illegal activities or activities otherwise prohibited, etc.
 - On-line games.
 - Proxy avoidance sites (or similar capabilities), such as 3Proxy, Unblockme, and Proxite.
 - Peer-to-peer (P2P) file sharing.

#

Exhibit 10.8.27-1 (Cont. 1) (09-12-2024)**Prohibited Uses of Government Furnished IT Equipment and Resources**

Note: P2P file sharing refers to any software or system allowing individual users of the Internet, intranet or extranet to connect and share files or resources. Participating in P2P file sharing creates a substantial computer security risk, and must facilitate the spread of computer viruses.

7. Individuals must not subscribe to unofficial LISTSERV or other services (e.g., retailers, recipes, coupon distributors) which creates a high volume of email traffic.
8. Individuals must not create, copy, transmit, download, store, or retransmit prohibited materials, video, or sound (such as streaming video or music).

Note: The allowance of streaming media (video or music) is to be done only when based on a justifiable, IRS manager-approved business need.

9. Individuals must not download, copy, or install unauthorized applications or data programs (e.g., executable code), such as: (Refer to Exhibit 10.8.27-2 for definition of an unauthorized data program)
 - Screen savers.
 - Software products.
 - "Push" technology applications (subscriber services) from the Internet (e.g., weather or news alert feeds, stock quote updates) that gather information and send it out automatically to a subscriber.
 - Test or demo software.
 - Computer games.
10. Individuals are prohibited from using social media (e.g., Google Groups, Facebook, Instagram, Second Life, Flickr, Twitter, Snapchat, TikTok) in an official capacity, or during their duty time, and such use must be separate from their job.

Note: An exception has been made for approved IRS communicators working on official IRS media initiatives. Refer to IRM 11.1.3, *Communications, Contact with the Public and the Media*, for guidance on authorized usage of new media and social media tools.

11. Individuals are specifically prohibited from engaging in any political fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity. Individuals are also prohibited from using government furnished IT equipment and resources for any of the aforementioned activities.
12. Individuals are prohibited from the unauthorized acquisition, use, reproduction, transmission, or distribution of controlled information including computer software and data, that includes privacy information; material which is copyrighted, trademarked, or otherwise controlled with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

Note: Copyrighted materials include, but are not limited to, music, videos, and pictures.

13. Individuals must not participate in activities that are illegal, inappropriate, or offensive to fellow employees, contractors, vendors, outsourcing providers, or the public in general. Such activities include, but are not limited to, hate speech, or material that ridicules others on the basis of age, race, creed, religion, color, sex, disability, national origin, or sexual orientation.
14. Individuals must not post agency information whether using government furnished IT equipment and resources, or personal resources to external news groups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless the appropriate agency written approval has been obtained or the use is not at odds with the agency's mission or positions.
15. Individuals are prohibited from storing personal information/files within Home Directories or other network drives provided and maintained by the IRS.
16. Individuals are prohibited from engaging in any use of government furnished IT equipment and resources that reduces employee productivity or interferes with the performance of official duties.
17. Individuals are prohibited from accessing or syncing non-IRS email and calendar accounts through the Internet (e.g., Yahoo, corporate, other Federal/State/Local/Tribal).
18. Individuals are prohibited from the inappropriate use of IRS email account(s), such as:
 - Transmitting files larger than the specified size (Refer to IRM 1.10.3, *Office of the Commissioner of*

Exhibit 10.8.27-1 (Cont. 2) (09-12-2024)**Prohibited Uses of Government Furnished IT Equipment and Resources**

Internal Revenue, Standards for Using Email) .

- Any correspondence for personal gain (Avon, private commercial business, selling of personal goods or services, etc.).
 - Solicitation of individuals, such as Girl Scout or Boy Scout fundraisers.
 - Chain letters or other unauthorized mass mailings regardless of the subject matter.
19. Individuals are prohibited from accessing the Internet without using an IRS-approved VPN connection.
 20. Individuals are prohibited from accessing any Internet site that contains similar content to sites which have been prohibited or restricted.
 21. Individuals are prohibited from using government furnished equipment (e.g., copier, fax machine) to make more than a few copies of material (e.g., copying a book, making numerous copies of a resume, or sending/receiving a lengthy document via fax machines), as well as any use of such machines that conflicts with the actual need to use the government furnished equipment for official business purposes.
 22. Individuals are prohibited from using telephone services when such use will create more than a minimal additional expense to the government.

Exhibit 10.8.27-2 (09-12-2024)**Terms and Acronyms**

Term	Definition
AO	Authorizing Official
CISA	Cyberbersecurity and Infrastructure Security Agency
CMMI	Capability Maturity Model Integration
EFC	Enterprise FISMA Compliance
ELC	Enterprise Life Cycle
Employee non-duty time	<p>Times when the individual is not otherwise expected to be addressing official business. Individuals must, for example, use government furnished IT equipment and resources during their non-duty time such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).</p> <p>For individuals using government furnished IT equipment and resources in a government facility, no expanded access to the building will be provided beyond when the building is normally open for access. The use of government furnished IT equipment and resources during the aforementioned periods must be determined and/or agreed to by the individual and the organization's managers.</p>
EO	Executive Order
FISMA	Federal Information Security Modernization Act of 2014
Government furnished IT equipment and resources	Includes, but is not limited to, office and telephone equipment and services (e.g., phone sets, cell phones, Blackberries, pagers, tablets, and voice mail), desktop and laptop computers. It also includes related peripheral equipment (e.g., printers, scanners) and application software, library resources, fax machines, and photocopiers.

Personal Use of Government Furnished Information Technology Equipment and Resources 10.8.27

page 11

Exhibit 10.8.27-2 (Cont. 1) (09-12-2024)

Terms and Acronyms

Term	Definition
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: <ol style="list-style-type: none">1. Requires the use of such equipment; or2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.
ITIL	Information Technology Infrastructure Library
Limited Personal Use	Activity by individuals that is conducted during personal time in the course of the business day and is considered an "authorized use" of government furnished property as the term is used in the Standards of Conduct for Employees of the Executive Branch (5 CFR §2635.101 (b) (9) and §2635.704 (a)).
LSS	Lean Six Sigma

Exhibit 10.8.27-2 (Cont. 2) (09-12-2024)**Terms and Acronyms**

Term	Definition
Minimal additional expense	An individual's limited personal use of government furnished IT equipment and resources is confined to those situations where the government is already providing resources or services, and the use of such resources or services will not result in any additional expense to the government, will result in only fair wear and tear, or use of small amounts of electricity, ink, toner, or paper. Examples of minimal additional expenses include: making a few photocopies, using a computer printer to print out a few pages of material, making occasional brief personal phone calls (within Treasury Department policy), infrequently sending personal email messages, or limited use of the Internet for personal reasons. Limited personal use activity by individuals that is conducted during personal time in the course of the business day is considered an "authorized use" of government furnished IT equipment and resources as the term is used in the Standards of Conduct for Employees of the Executive Branch (5 CFR § 2635.101 (b) (9) and § 2635.704 (a)).
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
Personally Identifiable Information (PII)	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.) (OMB Circular A-130, NIST SP 800-122).

Exhibit 10.8.27-2 (Cont. 3) (09-12-2024)

Terms and Acronyms

Term	Definition
Privilege	In the context of this policy, means that the IRS is extending the opportunity to its employees, contractors, vendors, and outsourcing providers, to use government furnished IT equipment and resources for limited personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use government furnished IT equipment and resources for non-government purposes. Nor does the privilege extend to modifying the equipment used, including loading personal software, copying existing software, or making configuration changes.
Risk-Based Decisions (RBD)	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive).
Sensitive But Unclassified (SBU)	Originated with the Computer Security Act of 1987. It is defined as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC) (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy." (TD P 15-71)
SOP	Standard Operating Procedure
SP	Special Publication
SRM	Security Risk Management
TD	Treasury Directive

Exhibit 10.8.27-2 (Cont. 4) (09-12-2024)
Terms and Acronyms

Term	Definition
Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program	In accordance with the Taxpayer Browsing Protection Act (Public Law No. 105-35), the IRS created the unauthorized access or inspection of tax information and records (UNAX) program to implement privacy protection and statutory unauthorized access and browsing prevention requirements.
Unauthorized data program	A program not explicitly approved or permitted by the organization(s) with responsibility for managing data programs.

Exhibit 10.8.27-3 (09-12-2024)**Related Resources**

IRS Publications

- IRM 1.10.3, *Office of the Commissioner of Internal Revenue, Standards for Using Email*
- IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*
- IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*
- IRM 10.8.26, *Information Technology (IT) Security, Wireless and Mobile Device Security Policy*
- IRM 10.9.1, *Classified National Security Information*
- IRM 11.1.3, *Communications, Contact with the Public and the Media*
- IRM 11.3.1, *Disclosure of Official Information, Introduction to Disclosure*
- Publication 4812, *Contractor Security & Privacy Controls*

Department of the Treasury Publications

- TD 81-01, *Treasury Information Technology (IT) Programs*, July 14, 2009
- TD P 15-71, *Department of the Treasury Security*, June 17, 2011
- TD P 85-01, Version 3.1.3 *Treasury Information Technology (IT) Security Program*, February 28, 2022
- TD 87-04, *Personal Use of Government Information Technology Resources*, January 27, 2012

Other Publications

- 5 CFR § 2635.101 (b) (5) and (9), *Basic Obligation of Public Service*
- 5 CFR § 2635.702 (b), *Appearance of Governmental Sanction*
- 5 CFR § 2635.704 (a) and (b) (1), *Use of Government Property*
- 5 CFR § 2635.705, *Use of Official Time*
- 5 CFR § 735.203, *Conduct Prejudicial to the Government*
- 5 CFR Part 3101, *Supplemental Standards Of Ethical Conduct For Employees Of The Department Of The Treasury*
- 31 CFR Part 0, *Department Of The Treasury Employee Rules Of Conduct*
- 31 CFR § 0.218, *General Conduct Prejudicial to the Government*
- IRM 6.735.2, *Ethics and Conduct Matters*
- Federal CIO Council, *Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment including Information Technology*, May 19, 1999
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, November 8, 2000
- OMB Memorandum for Chief Acquisition Officers, *Revisions to the Federal Acquisition Certification for Contracting Officer's Representatives (FAC-COR)*, September 6, 2011 Public Law 103-94, The Hatch Act Reform Amendment of 1993, October 6, 1993
- OMB Memorandum 23-13, *"No TikTok on Government Devices" Implementation Guidance*, February 27, 2023
- Public Law 103-94, *The Hatch Act Reform Amendment of 1993*, October 6, 1993
- Public Law 113-283, *Federal Information Security Modernization Act of 2014*, December 18, 2014
- IRS IT Organization: <http://it.web.irs.gov/ProceduresGuidelines/ITNameChange.htm>

