



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.27

JUNE 20, 2017

## EFFECTIVE DATE

(06-20-2017)

## 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) The following revisions have been made to this version of policy:
  - a. Restructured IRM introductory titles and layout in accordance with IRM 1.11.2, *Internal Management Documents System, Internal Revenue Manual (IRM) Process*.
  - a. Updated the following sections:
    - IRM Section 10.8.27.1, Overview
    - IRM Section 10.8.27.1.4, Risk Acceptance and Risk-Based Decisions
    - IRM Exhibit 10.8.27-1, Prohibited Uses of Government Furnished IT Equipment and Resources
    - IRM Exhibit 10.8.27-2, Glossary
    - IRM Exhibit 10.8.27-3, References
  - b. Updated organizational links throughout the document.
- (2) Replaced “government IT resources” throughout, with “government furnished IT equipment and resources” to provide clarification and ensure consistency with policies in the IRM 10.8.x series.
- (3) Removed all references to IRM 10.8.3, *IT Security, Audit Logging Security Standards*, as the IRM is now obsolete; all Security Policy managed auditing requirements are now located in IRM 10.8.1, *IT Security, Policy and Guidance*.
- (4) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM.

## EFFECT ON OTHER DOCUMENTS

IRM 10.8.27 dated September 29, 2014, is superseded. This IRM supersedes all prior versions of IRM 10.8.27. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.

## AUDIENCE

IRM 10.8.27 shall be distributed to all personnel responsible for ensuring proper use and security of IRS equipment, resources, information, and information systems.

S. Gina Garza  
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 Scope

#### 10.8.27.1.2 Objectives

#### 10.8.27.1.3 Background

#### 10.8.27.1.4 Authority

#### 10.8.27.1.5 Risk Acceptance and Risk-Based Decisions

### 10.8.27.2 Roles and Responsibilities

#### 10.8.27.2.1 Agency Head

#### 10.8.27.2.2 Associate Chief Information Officer (ACIO), Cybersecurity

#### 10.8.27.2.3 Contracting Officer's Representative (COR)

#### 10.8.27.2.4 Employees

#### 10.8.27.2.5 IRS Information Technology (IT) Organization

#### 10.8.27.2.6 Managers

### 10.8.27.3 Specific Requirements

## Exhibits

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

### 10.8.27-2 Glossary and Acronyms

### 10.8.27-3 References



10.8.27.1  
(06-20-2017)  
**Program Scope and  
Objectives**

- (1) This IRM lays the foundation to implement and manage security for the personal use of government furnished Information Technology (IT) equipment and resources for non-government purposes within the IRS.
- (2) **Audience:** This IRM applies to all employees, contractors, vendors, and volunteers of the IRS.
- (3) **Policy Owner:** Gina Garza, Chief Information Officer.
- (4) **Program Owner:** Olga Plotkin, Program Manager, Cybersecurity, Security Policy.

10.8.27.1.1  
(06-20-2017)  
**Scope**

- (1) This IRM provides guidance for the allowable minimum standard regarding the acceptable personal use of government furnished IT equipment and resources by IRS employees, contractors, vendors, and outsourcing providers.

**Note:** The following circumstances are addressed in this policy:

- a. Minimum allowable usage of government furnished IT equipment and resources
  - b. Prohibited usage of government furnished IT equipment and resources
  - c. Roles and Responsibilities
  - d. Tour of Duty (TOD) Hours
  - e. Non-Duty Hours
  - f. Performing work for the Department of the Treasury, its offices, and bureaus
- (2) The provisions in this manual 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 information systems that store, process, or transmit IRS information or connect to an IRS network or system.
    - c. All IRS information and information systems. For information systems that store, process, or transmit classified information, please refer to IRM 10.9.1, *National Security Information*, for additional procedures for protecting classified information.

10.8.27.1.2  
(06-20-2017)  
**Objectives**

- (1) This IRM establishes the minimum baseline security policy and requirements for all IRS Information Technology (IT) assets in order 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.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive controls requires a risk-based decision. See the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

10.8.27.1.3  
(06-20-2017)  
**Background**

- (1) The expanding use of IT resources to a growing group of IRS employees in the workplace, increasingly offers new opportunities to meet the Internal Revenue Service's (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 information systems and infrastructure.
- (2) IRM 10.8.27 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.27.1.4  
(06-20-2017)  
**Authority**

- (1) IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, establishes the security program and the policy framework for the IRS.
- (2) Federal Information Processing Standards Publication (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as an initial set of baseline security controls for the creation of agency IT security policy.
- (3) 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 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

10.8.27.1.5  
(06-20-2017)  
**Risk Acceptance and  
Risk-Based Decisions**

- (1) Any exception to this policy requires that the Authorizing Official (AO) make a Risk-Based Decision.
- (2) Risk-Based Decision requests shall be submitted in accordance with IRM 10.8.1 and use of Form 14201, as described in the Risk Acceptance Request and Risk-Based Decision standard operating procedures (SOP), available on the Enterprise Federal Information Security Management Act (FISMA) Compliance SharePoint site via the Risk Acceptance Requests link at: <https://portal.ds.irsnet.gov/sites/CyberSRM/SitePages/RiskDecisions.aspx>.
- (3) Refer to IRM 10.8.1 for additional guidance about risk acceptance.

10.8.27.2  
(06-20-2017)  
**Roles and  
Responsibilities**

- (1) IRM 10.8.2 *Information Technology Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and computer security, and is the authoritative source for such information.
- (2) The supplemental roles and responsibilities provided below are specific to the implementation of security for the personal use of government furnished IT equipment and resources for non-government purposes.

10.8.27.2.1  
(09-29-2014)  
**Agency Head**

- (1) The E-Government Act of 2002 (P.L. 107-347) Title III and the Federal Information Security Management Act of 2002, require the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of its information and information systems. These protections not only apply to employees within the agency, but also to contractors, and/or other organizations working on behalf of the agency, as defined in IRM 10.8.2.
- (2) The IRS's Agency Head is the Commissioner; the Commissioner shall be responsible for ensuring that this policy is disseminated to all employees.

10.8.27.2.2  
(09-29-2014)  
**Associate Chief  
Information Officer  
(ACIO), Cybersecurity**

- (1) The Associate Chief Information Officer (ACIO), Cybersecurity, shall develop and disseminate additional policy appropriate to personal use as necessary.

10.8.27.2.3  
(06-20-2017)  
**Contracting Officer's  
Representative (COR)**

- (1) The Contracting Officer's Representative (COR) shall ensure contractors are informed of appropriate uses of government furnished IT equipment and resources as a part of their introductory training, orientation, or the initial implementation of this policy.
- (2) The COR shall ensure IT resources are being used appropriately and shall take corrective action if needed.
- (3) The COR shall ensure contractors who process, store, or transmit IRS information on government furnished equipment, software and media, do so only when the contract under which they perform, specifically establishes terms and conditions for such use (and that appropriate approvals have been obtained), and the contractor otherwise meets and complies with the security standards detailed in IRM 10.8.1, the contract, Publication 4812, and/or other applicable IRS policy guidance.

10.8.27.2.4  
(06-20-2017)  
**Employees**

- (1) While using government furnished IT equipment and resources, individuals shall be responsible for their own personal and professional conduct and shall follow, among others, the rules and regulations described below:
  - a. Do not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the government. (5 CFR § 735.203)
  - b. Put forth honest effort in the performance of their duties. (5 CFR § 2635.101(b)(5))

- c. Do not use or permit the use of their government position or title, or government furnished IT equipment and resources, or any authority associated with their public office in a manner that could reasonably be construed to imply that their agency or the government sanctions or endorses their personal activities. (5 CFR § 2635.702(b))
- d. Protect and conserve government property and shall not use such property, or allow its use, for any unauthorized purposes. (5 CFR § 2635.101(b)(9))

**Note:** Employee conduct pursuant to this policy is considered an authorized use of government property as the term is used in 5 CFR § 2635.704(a). See TD 87-04,(4)(e)Appendix A(e), Definitions (defining limited personal use).

- e. Use official-time in an honest effort to perform official duties and in accordance with law or regulation (5 CFR § 2635.705(a)).
- f. Ensure that they do not give the false impression that they are acting in an official capacity when they are using government furnished IT equipment and resources for non-government purposes. In addition, they shall not post, disseminate, or otherwise use IRS documents and/or symbols as part of personal documents, Internet sites, or other forms of communication. (IRS-defined)

**Note:** If there is an expectation that such a personal use could be interpreted to represent an agency, an adequate disclaimer must be used. One acceptable disclaimer is - "The content of this message does not reflect the position of the U.S. Government, the Department of the Treasury, or the IRS."

10.8.27.2.5  
(09-29-2014)  
**IRS Information  
Technology (IT)  
Organization**

- (1) The IRS IT organization is responsible for maintenance and dissemination of this policy, and shall establish sufficient controls to ensure equipment is used appropriately.

10.8.27.2.6  
(06-20-2017)  
**Managers**

- (1) Managers shall ensure individuals are informed of appropriate uses of government furnished IT equipment and resources as a part of their introductory training, orientation, and/or the initial implementation of this policy. These requirements are also part of IRS employees' mandatory annual Security Awareness Training and Education (SATE).
- (2) Managers shall ensure IT resources are being used appropriately and shall take corrective action if needed.

10.8.27.3  
(06-20-2017)  
**Specific Requirements**

- (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 <http://www.irs.gov/Individuals/1040-Central> for IRS employees to look up their own tax information. These tools and applications are considered to be external. Examples of these tools include:
  - Where's My Refund?
  - Get Transcript of Your Tax Records
  - Do I Qualify for EITC?
  - Various forms and instructions for filing, etc.



- (2) Individuals should have no expectation of privacy while using any government furnished IT equipment and resources at anytime, including (but not limited to) accessing the Internet, proxy avoidance server, or email. Individuals should 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 should avoid using government furnished IT equipment and resources such as their computer, the Internet or email.
  - a. See the IRM 10.8.1, section “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 shall 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 shall 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 10.8.26, *Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Device Security Policy.*
- Any other IRS privacy concerns related to the safeguarding of agency information.

**Exhibit 10.8.27-1 (06-20-2017)****Prohibited Uses of Government Furnished IT Equipment and Resources**

Regardless of work status, individuals should 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. See the UNAX web site for additional guidance on unauthorized access to tax information. <http://irweb.irs.gov/AboutIRS/bu/pipds/pip/privacy/unax/default.aspx>.
2. In accordance with IRM 1.10.3 , *Office of the Commissioner of Internal Revenue, Standards for Using Email* and IRM 11.3.1 , *Introduction to Disclosure*, individuals shall 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. For details, see the interim guidance PGLD-10-0616-0003, **Using IRS and Personal Email Accounts** (to be incorporated into the Email section of IRM 10.5.1 **Privacy Policy**).
- 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. See IRM 10.5.1, *Privacy Policy*, for additional guidance pertaining to emailing SBU (including PII) with personal accounts.
3. Individuals shall 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 may 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 shall 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 information 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) (06-20-2017)****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 may facilitate the spread of computer viruses.

7. Individuals shall not subscribe to unofficial LISTSERV or other services (e.g., retailers, recipes, coupon distributors) which creates a high volume of email traffic.
8. Individuals shall 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 shall not download, copy, or install unauthorized applications or data programs (e.g., executable code), such as: (See 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, MySpace, Facebook, Instagram, Second Life, Flickr, Twitter) in an official capacity, or during their duty time, and such use shall be separate from their job.

**Note:** An exception has been made for approved IRS communicators working on official IRS media initiatives. See 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 shall 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 shall 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).

**Exhibit 10.8.27-1 (Cont. 2) (06-20-2017)****Prohibited Uses of Government Furnished IT Equipment and Resources**

18. Individuals are prohibited from the inappropriate use of IRS email account(s), such as:
  - Transmitting files larger than the specified size (see <http://irweb.irs.gov/AboutIRS/Nwsctr/Headlines/32760.aspx>).
  - 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 fund raisers.
  - 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 (06-20-2017)****Glossary and Acronyms**

**Employee non-duty time** - Times when the individual is not otherwise expected to be addressing official business. Individuals may, 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). 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 should be determined and/or agreed to by the individual and the organization's managers.

**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 photocopyers.

**Information Technology** - 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:

1. Requires the use of such equipment; or
2. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

**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)).

**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)).

**Personally Identifiable Information (PII)** - All taxpayer information or any combination of information that can be used to uniquely identify, contact, or locate a person. A specific type of sensitive and SBU information that includes the personal information of taxpayers, and the personal information of employees, contractors, applicants, and visitors to the IRS. Examples of PII include, but are not limited to: name; home address; Social Security number; date of birth; home telephone number; biometric data (e.g., height, weight, eye color, fingerprints, etc.); and other numbers or information that alone or in combination with other data can identify an individual.

**Exhibit 10.8.27-2 (Cont. 1) (06-20-2017)****Glossary and Acronyms**

**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.

**Sensitive But Unclassified (SBU)** - Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or to the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.

**Unauthorized data program** - Is a program not explicitly approved or permitted by the organization(s) with responsibility for managing data programs.



**Exhibit 10.8.27-3 (09-29-2014)****References**

The following references were used in developing this policy:

- a. 5 CFR § 2635.101 (b) (5) and (9), *Basic Obligation of Public Service*
- b. 5 CFR § 2635.702 (b), *Appearance of Governmental Sanction*
- c. 5 CFR § 2635.704 (a) and (b) (1), *Use of Government Property*
- d. 5 CFR § 2635.705, *Use of Official Time*
- e. 5 CFR § 735.203, *Conduct Prejudicial to the Government*
- f. 5 CFR Part 3101, *Supplemental Standards Of Ethical Conduct For Employees Of The Department Of The Treasury*
- g. 31 CFR Part 0, *Department Of The Treasury Employee Rules Of Conduct*
- h. 31 CFR § 0.213, *General Conduct Prejudicial to the Government*
- i. Federal CIO Council, *Recommended Executive Branch Model Policy/Guidance on "Limited Personal Use" of Government Office Equipment including Information Technology*, May 19, 1999
- j. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- k. OMB Memorandum for Chief Acquisition Officers, *Revisions to the Federal Acquisition Certification for Contracting Officer's Representatives (FAC-COR)*, September 6, 2011
- l. The Hatch Act Reform Amendment of 1993, P.L. 103-94
- m. TD 81-01, *Department of the Treasury Information Technology (IT) Manual*, July 14, 2009
- n. TD P 85-01, *Department of the Treasury IT Security Program*, April 28, 2014
- o. TD 87-04, *Personal Use of Government Information Technology Resources*, January 27, 2012
- p. IRM 1.10.3, *Office of the Commissioner of Internal Revenue, Standards for Using Email*
- q. IRM 6.751.1, *Discipline and Disciplinary Actions, Policies, Responsibilities, Authorities, and Guidance*, Exhibit 6.751.1-1
- r. IRM 10.8.1, *IT Security, Policy and Guidance*
- s. IRM 10.8.2, *IT Security, IT Security Roles and Responsibilities*
- t. IRM 10.8.26, *Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Device Security Policy*
- u. IRM 10.8.40, *IT Security, Wireless Security Policy*
- v. IRM 10.9.1, *National Security Information*
- w. IRM 11.1.3, *Communications, Contact with the Public and the Media*
- x. IRWeb link: <http://irweb.irs.gov/AboutIRS/Nwsctr/Headlines/32760.aspx>
- y. IRS IT organization website: <http://it.web.irs.gov/ProceduresGuidelines/ITNameChange.htm>