EFFECTIVE DATE

(11-06-2023)

PURPOSE

(1)   This transmits the revised IRM 10.8.26, *Information Technology (IT) Security, Wireless and Mobile Device Security Policy*.

MATERIAL CHANGES

(1)   IRM 10.8.26.1 updated to align with IRM 1.11.2, Internal Management Documents System, Internal Revenue Manual (IRM) Process Internal Controls.

(2)   Removed example references of Blackberry UEM throughout the IRM.

(3)   Added example references of Microsoft Intune Company Portal throughout the IRM.

(4)   Editorial changes (including grammar, spelling, and clarification) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.26 dated April 25, 2022, is superseded. This IRM supersedes all prior versions of IRM 10.8.26, and supplements: IRM 10.8.1, *IT Security, Policy and Guidance* and IRM 10.8.2, *IT Security, IT Security Roles and Responsibilities*.

AUDIENCE

IRM 10.8.26 applies to and shall be distributed to all employees, contractors, vendors, and volunteers responsible for ensuring the security of government furnished mobile devices and approved non-government furnished/personally owned (BYOD) mobile devices.

Kaschit Pandya
Acting, Chief Information Officer

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26**
Any line marked with a #
is for **Official Use Only**

10.8.26
Wireless and Mobile Device Security Policy

Table of Contents

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26**
Any line marked with a #
is for **Official Use Only**

Exhibits

#

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26**
Any line marked with a #
is for **Official Use Only**

10.8.26.1 (11-06-2023) **Program Scope and Objectives**	(1)	**Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage security controls and guidance for government furnished mobile devices and non-government furnished/personally owned mobile devices that have been approved for use by employees participating in the Bring Your Own Device (BYOD) program, and the data stored on them, within the Internal Revenue Service (IRS).

(2) **Purpose of the Program**: Develop and publish policies to protect the IRS against potential Information Technology (IT) threats and vulnerabilities and ensure compliance with federal mandates and legislation.

(3) **Audience**: 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, volunteers and outsourcing providers, who use or operate information systems or mobile devices that store, process, or transmit IRS information or connect to an IRS network or system.

> *Note:* When the terms "mobile devices" and "mobile device users" are used within this IRM, they refer to both government furnished and approved non-government furnished/personally owned mobile devices and users unless otherwise noted.

c. Bring Your Own Device (BYOD) participants, unless otherwise specified as only government furnished mobile devices.
d. Government furnished or approved non-government furnished/personally owned mobile devices used to accomplish the IRS mission.

> *Note:* For the purpose of this IRM, laptops are categorized as a mobile device with computing and communication (e.g., wireless, local area network (LAN)) capability, and shall comply with all IRM 10.8.1, Treasury Directive Publication (TD-P) 85-01, and other related IRM policy requirements for mobile devices. (IRS-defined)

e. All IRS information and information systems. For information systems that store, process, or transmit, classified information, please refer to IRM 10.9.1, *Classified National Security Information (NSI)*, for additional procedures for protecting classified information.

(4) **Policy Owner**: Chief Information Officer.

(5) **Program Owner**: Cybersecurity Threat Response and Remediation (an organization within Cybersecurity)

(6) **Program Goals**: Cybersecurity Policy is responsible for the development and maintenance of IRS' enterprise IT security policies. The IRM 10.8.X series provides the minimum-security requirements to protect the confidentiality, integrity, and availability of data processed on IRS systems. IRMs are developed in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB), Treasury Directives (TDs), National Institute of Standards and Technology (NIST) publications, and National Achieves and Records Administration (NARA).

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.1**
Any line marked with a #
is for **Official Use Only**

10.8.26.1.1 (11-06-2023) **Background**	(1)	Government furnished and non-government furnished/personally owned mobile devices are vulnerable to theft and the loss of all data stored on them, which places the information they contain at risk of disclosure or compromise. Many theft rings operating today at airports, hotels, and other public places target mobile devices. Additionally, the use of mobile devices in public places (e.g., airports, restaurants, conferences, public transportation) and transmitting information through public telecommunications networks, presents a significant risk of unauthorized persons observing and gaining access to the information that is being processed. Therefore, IRS employees, contractors, and volunteers shall abide by all requirements provided within this policy to help protect their government furnished and non-government furnished/personally owned mobile devices, and the information contained on them, from these risks.
	(2)	The IRS has implemented the ″Bring Your Own Device″ (BYOD) program to permit IRS personnel to use non-government furnished/personally owned mobile devices for business purposes. This program offers the convenience of using an approved non-governmentfurnished/personally owned mobile device to access, process, transmit, or store IRS information. Therefore, those IRS employees who choose to participate in the program shall abide by the requirements specified within this policy. The IRS shall be able to ensure that agency data is protected at all places and all times.
	(3)	IRM 10.8.26 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRM Information Technology, Cybersecurity.
10.8.26.1.2 (11-06-2023) **Authority**	(1)	All IRS systems and applications shall be compliant 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.
10.8.26.1.3 (11-06-2023) **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
	(2)	The supplemental roles and responsibilities provided below are specific to the implementation of government and non-government/personally owned (BYOD) devices.
10.8.26.1.4 (04-25-2022) **Government Furnished Mobile Device Users**	(1)	Government furnished mobile device users shall be responsible for ensuring the physical and logical security of their assigned equipment. (IRS-defined)
	Note:	An example of how an employee shall ensure the logical security of a mobile device by exercising due care in preventing viruses and malware from being installed on their mobile devices by not opening attachments and documents from untrusted sources(i.e., attachments and documents from a personal email).
	(2)	Managers of employees who have been assigned government furnished mobile devices shall ensure their employees exercise due care in safeguarding these devices and the data they contain. (IRS-defined)

(3)   Refer to IRM 10.8.27, *Information Technology (IT) Security, Personal Use of Government Furnished Information Technology Equipment and Resources*, for guidance pertaining to the prohibited uses of government furnished mobile devices.

10.8.26.1.5
(11-06-2023)
Non-Government Furnished/Personally Owned (BYOD) Mobile Device Users

(1)   BYOD participants shall: (IRS-defined)

a.   Understand that if their approved non-government furnished/personally owned mobile device is not compliant with IRS security policies or if it presents any unacceptable risk to the IRS's networks or data, that it will not be allowed to connect to the IRS's systems.

b.   Consent to remote inspection and monitoring of the IRS-approved mobile access solution on their approved non-government furnished/personally owned mobile device, using technology centrally managed by IRS IT organization

c.   Ensure they are the only person who has access to their approved non-government furnished/personally owned mobile devices when being used to view or process IRS information.

d.   Ensure a valid password is successfully entered prior to logging onto the mobile device.

e.   Ensure a valid password is successfully entered prior to logging into the IRS-approved mobile access solution.

f.   See the Rules of Behavior for BYOD Participants section within this IRM for further requirements when using their approved non-government furnished/personally owned mobile device to access, process, transmit, or store IRS information.

(2)   BYOD participants shall *not*: (IRS-defined)

a.   Use the screen capture function on their mobile device while logged into the IRS-approved mobile access solution.

   Note: Using the screen capture function while logged into the IRS-approved mobile access solution, could place IRS sensitive information (e.g., Sensitive But Unclassified (SBU) and Personally Identifiable Information (PII)) at risk of disclosure.

b.   Share their IRS-approved mobile access solution password with anyone.

10.8.26.1.6
(11-06-2023)
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.X 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.

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**   Internal Revenue Manual   **10.8.26.1.6**

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, National Archives and Records Administration (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.

10.8.26.1.7
(11-06-2023)
Program Controls

(1) Each IRM in the 10.8.X series is assigned an author who reviews their IRM annually to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, DISA) for potential revisions to security policies and security requirement 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 requirement 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 include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, Classified National Security Information (NSI), for additional guidance for protecting classified information.

(4) This IRM establishes the minimum baseline security policy and requirements for all IRS wireless, mobile and BYOD devices and IRS-approved mobile access solutions 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.

(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.

10.8.26.1.8
(11-06-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.26-2 for a list of terms, acronyms, and definitions.

10.8.26.1.9
(11-06-2023)
Related Resources

(1) Refer to Exhibit 10.8.26-3 for a list of related resources and references.

10.8.26.2
(11-06-2023)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this policy requires that the Authorizing Official (AO) make a RBD

10.8.26.1.7   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

(2)   Users shall submit RBD requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process within the Risk Based Decision Standard Operating Procedures (SOP).

#
#
#
#

(3)   Refer to IRM 10.8.1 for additional guidance about risk acceptance.

10.8.26.3 (04-25-2022) **IT Security Controls**	(1) The IT security controls within this manual provide a range of safeguards and countermeasures for the government furnished and approved non-government furnished/personally owned mobile devices that access, process, transmit, or store IRS information.

(2)   The security controls in this IRM supplement the requirements found in IRM 10.8.1.

(3)   Refer to IRM 10.8.1 for security control families and security controls not addressed within this IRM.

10.8.26.3.1
(04-25-2022)
AC - Access Control

(1)   In addition to the Access Control guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1

- AC-1 Access Control Policy and Procedures
- AC-4 Information Flow Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege
- AC-13 Withdrawn by NIST
- AC-14 Permitted Actions without Identification or Authentication
- AC-15 Withdrawn by NIST
- AC-16 Security and Privacy Attributes
- AC-20 Use of External Systems
- AC-21 Information Sharing
- AC-22 Publicly Accessible Content
- AC-23 Data Mining Protection
- AC-24 Access Control Decisions
- AC-25 Reference Monitor

10.8.26.3.1.1
(04-25-2022)
AC-2 Account Management

(1)   The UEM server shall provide automated mechanisms for supporting account management functions. (DISA UEM Server SRG: SRG-APP-000023-UEM-000012)

(2)   The UEM server shall automatically remove or disable temporary user accounts, in accordance with IRM 10.8.1, if supported by the UEM server. (DISA UEM Server SRG: SRG-APP-000024-UEM-000013)

(3)   The UEM server shall automatically disable accounts after a period of account inactivity, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000025-UEM-000014)

(4)   The UEM server shall automatically audit account creation. (DISA UEM Server SRG: SRG-APP-000026-UEM-000015)

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.1.1**
Any line marked with a #
is for **Official Use Only**

(5)   The UEM server shall automatically audit account modification. (DISA UEM Server SRG: SRG-APP-000027-UEM-000016)

(6)   The UEM server shall automatically audit account disabling actions. (DISA UEM Server SRG: SRG-APP-000028-UEM-000017)

(7)   The UEM server shall automatically audit account removal actions. (DISA UEM Server SRG: SRG-APP-000029-UEM-000018)

(8)   The UEM server shall notify system administrators and the Information System Security Officer (ISSO) when accounts are created. (DISA UEM Server SRG: SRG-APP-000291-UEM-000165)

(9)   The UEM server shall notify administrators and the ISSO when accounts are modified. (DISA UEM Server SRG: SRG-APP-000292-UEM-000166)

(10) The UEM server shall notify system administrators and the ISSO for account disabling actions. (DISA UEM Server SRG: SRG-APP-000293-UEM-000167)

(11) The UEM server shall notify system administrators and the ISSO for account removal actions. (DISA UEM Server SRG: SRG-APP-000294-UEM-000168)

(12) The UEM server shall automatically audit account-enabling actions. (DISA UEM Server SRG: SRG-APP-000319-UEM-000192)

(13) The UEM server shall notify system administrator and ISSO of account enabling actions. (DISA UEM Server SRG: SRG-APP-000320-UEM-000193)

(14) Refer to IRM 10.8.1 for additional guidance on Account Management.

10.8.26.3.1.2
(04-25-2022)
AC-3 Access
Enforcement

(1)   Mobile devices connected to IRS networks or processing IRS information shall comply with IRM 10.8.1 and the security requirements of those networks. (IRS-defined)

(2)   The UEM server shall employ an audited override of automated access control mechanisms under organization-defined conditions. (DISA UEM Server SRG: SRG-APP-000327-UEM-000200)

(3)   The UEM server shall be configured to have at least one user in defined administrator roles. (DISA UEM Server SRG: SRG-APP-000329-UEM-000202)

(4)   Refer to IRM 10.8.1 for additional guidance on Access Enforcement.

10.8.26.3.1.2.1
(04-25-2022)
Access to Sensitive
Information

(1)   Sensitive information (e.g., SBU and PII) shall not be downloaded to mobile devices. (IRS-defined)

a.   Government furnished laptops are the only exception to this requirement

(2)   Sensitive information (i.e., Federal Taxpayer Information (FTI)/ 6103 information) shall not be viewed or discussed on mobile devices in public places (e.g., airports, coffee shops, hospitals, malls, etc.). (IRS-defined)

(3)   Sensitive information stored or processed on a government furnished laptop shall be protected with the same requirements as hard-copy documents (e.g., markings, distribution, destruction) and in accordance with the requirements defined within IRM 10.8.1. (IRS-defined)

10.8.26.3.1.2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
                                                                  Any line marked with a #
                                                                  is for **Official Use Only**

(4) Only government furnished laptops may be used to access, process, transmit, or store classified data. (IRS-defined)

10.8.26.3.1.3 (04-25-2022) **AC-6 Least Privilege**	(1) The UEM server shall audit the execution of privileged functions. (DISA UEM Server SRG: SRG-APP-000343-UEM-000216)
	(2) Refer to IRM 10.8.1 for additional guidance on Least Privilege.
10.8.26.3.1.4 (04-25-2022) **AC-7 Unsuccessful Logon Attempts**	(1) The UEM server shall enforce the number of consecutive invalid logon attempts by a user during a specified time period, in accordance with IRM 10.8.1 (DISA UEM Server SRG: SRG-APP-000065-UEM-000036)
	(2) The UEM server shall be configured to lock accounts after a number of unsuccessful logon attempts within a specified timeframe, in accordance with IRM 10.8.1 (DISA UEM Server SRG: SRG-APP-000345-UEM-000218)
	(3) Refer to IRM 10.8.1 for additional guidance on Unsuccessful Logon Attempts.
10.8.26.3.1.5 (04-25-2022) **AC-8 System-Use Notifications**	(1) The UEM server shall display the Standard Mandatory IRS System Use Notification Banner, in accordance with IRM 10.8.1, before granting access to the application. (DISA UEM Server SRG-APP-000068-UEM-000037)
	(2) The UEM server shall retain the access banner until the user acknowledges acceptance of the access conditions. (DISA UEM Server SRG. SRG-APP-000069-UEM-000038)
	(3) Refer to IRM 10.8.1 for additional guidance on System-Use Notifications.
10.8.26.3.1.6 (04-25-2022) **AC-9 Previous Logon (Access) Notification**	(1) The UEM server shall notify the user, upon successful logon (access) to the application, of the date and time of the last logon (access). (DISA UEM Server SRG: SRG-APP-000075-UEM-000041)
	(2) The UEM server shall notify the user, upon successful logon (access), of the number of unsuccessful logon (access) attempts since the last successful logon (access). (DISA UEM Server SRG: SRG-APP-000076-UEM-000042)
	(3) Refer to IRM 10.8.1 for additional guidance on Previous Logon (Access) Notification.
10.8.26.3.1.7 (04-25-2022) **AC-10 Concurrent Session Control**	(1) The UEM server shall limit the number of concurrent sessions per privileged user account to three or less concurrent sessions. For High System, the UEM server shall limit the number of concurrent sessions in accordance with IRM 10.8.1 (DISA UEM Server SRG: SRG-APP-000001-UEM000001)
	(2) Refer to IRM 10.8.1 for additional guidance on Concurrent Session Control.
10.8.26.3.1.8 (04-25-2022) **AC-11 Device Lock**	(1) The UEM server shall conceal, via the session lock, information previously visible on the display with a publicly viewable image. (DISA UEM Server SRG: SRG-APP-000002-UEM-000002)
	(2) The UEM server shall initiate a session lock after a period of inactivity, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000003-UEM-000003)

(3)   The Mobile Device Management (MDM) server shall provide the capability for users to directly initiate a session lock. (DISA UEM Server SRG: SRG-APP-000004-UEM-000004)

(4)   The MDM server shall retain the session lock until the user reestablishes access using established identification and authentication procedures. (DISA UEM Server SRG: SRG-APP-000005-UEM-000005)

(5)   Refer to IRM 10.8.1 for additional guidance on Device Lock.

10.8.26.3.1.9
(04-25-2022)
AC-12 Session Termination

(1)   The UEM server shall automatically terminate a user session after a period of inactivity, a accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000296-UEM-000170)

(2)   The UEM server shall provide logout capability for user-initiated communication sessions. (DISA UEM Server SRG: SRG-APP-000296-UEM-000170)

(3)   The UEM server shall display an explicit logout message to users indicating the reliable termination of authenticated communications sessions. (DISA UEM Server SRG: SRG-APP-000297-UEM-000171)

(4)   Refer to IRM 10.8.1 for additional guidance on Session Termination.

10.8.26.3.1.10
(11-06-2023)
AC-17 Remote Access

(1)   Remote access shall only be accomplished with a government furnished mobile device via an IRS-approved Virtual Private Network (VPN) solution that uses FIPS 140-validated encryption technology. (IRS-defined)

#
#
#

(3)   The UEM server shall use Transport Layer Security (TLS) 1.2, or higher, to protect the confidentiality of sensitive data during electronic dissemination using remote access. (DISA UEM Server SRG: SRG-APP-000014-UEM-000009)

(4)   The UEM server shall be configured to prohibit client negotiation to TLS 1.1, TLS 1.0, Secure Sockets Layer (SSL) 2.0, or SSL 3.0. (DISA UEM Server SRG: SRG-APP-000560-UEM-000394)

(5)   Refer to IRM 10.8.1 for additional guidance on Remote Access.

10.8.26.3.1.11
(04-25-2022)
AC-18 Wireless Access

(1)   IRS employees shall be responsible to ensure they only use the secured Wi-Fi (e.g. hotels, home): (IRS-defined)

Note: The intent of this requirement is to avoid a situation where the employee is inadvertently using their neighbors Wi-Fi.

#
#
#
#
#
#

10.8.26.3.1.9   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

(2) IRS employees are permitted to utilize secure Public Wi-Fi access (e.g., hospital, Internet café, coffee shop, public library). (IRS-defined)

(3) Use of Government Furnished Equipment (GFE) phones and GFE MiFi's/Hot-Spots for remote access to IRS IT assets (e.g., networks, systems) shall be provided through an encryption mechanism such as a virtual private network (VPN) connection that meets FIPS 140 validation requirements (AC-17(2)_T.206).

    a.   A Two factor authentication shall be implemented for all remote access to an IRS system (AC-17_T.006). Refer to IRM 10.8.1 for further guidance.

(4) Personally owned or contractor owned Commercial Mobile Devices (CMDs) shall not be used to transmit, receive, store, or process IRS information or connect to IRS networks without AO authorization. (IRS-defined)

(5) Privately owned Ethernet to Wi-Fi converters (e.g., wireless Ethernet bridges, wireless media adapters) shall not be connected to IRS laptops or workstations. (IRS-defined)

(6) Refer to IRM 10.8.1 for additional guidance on Wireless Access.

10.8.26.3.1.12
(11-06-2023)
AC-19 Access Controls
for Mobile Devices

(1) Mobile devices shall be provisioned with Public Key Infrastructure (PKI) digital certificates, in accordance with IRM 10.8.52, *IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*, so users can digitally sign and encrypt email notifications or other email messages required by IRS policy. (IRS-Defined)

                                                                                   #
  #
  #

    b.   AO approval shall be obtained prior to the use of software PKI certificates on mobile devices. (IRS-defined)

(2) IRS or Treasury-issued software certificates shall not be used for non-government furnished/personally owned mobile devices, unless they have been approved for use in the BYOD program. (DISA: SRG-MPOL-058; IRS-defined)

(3) Refer to IRM 10.8.1 for additional guidance on Access Control for Mobile Devices.

10.8.26.3.1.12.1
(07-21-2020)
Travel

(1) Travel requirements pertaining to Mobile Devices shall be implemented in accordance with AC-19 Access Control for Mobile Devices in IRM 10.8.1.

(2) For the purpose of requirements pertaining to overseas or foreign (international) travel with a government furnished mobile device (e.g., laptop, tablet, smartphone) the following apply: (IRS-defined)

    a.   IRS personnel permanently stationed overseas are not considered foreign travelers for the purpose of this section.
    b.   For IRS employees at U.S. diplomatic facilities abroad, U.S. Department of State requirements prevail for all IT security requirements in lieu of this IRM and TD-P 85-01.

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.1.12.1**
Any line marked with a #
is for **Official Use Only**

       c.   The IRS Tax Attaché' with responsibility for the country an employee is traveling to, may advise them of further restrictions for bringing laptops within their jurisdictions.

Note: The term ″U.S.″ is used here to refer to the United States, its possessions, and territories. "Non-U.S. Support" is used here to mean use of contractors or other non-Federal service providers located outside the U.S., its possessions, and territories.

10.8.26.3.1.12.2
(04-25-2022)
Access Controls for Government Furnished Mobile Devices

(1) Government furnished mobile devices shall not be used by anyone other than authorized personnel (e.g., the person to whom it is assigned, IT personnel performing maintenance/repairs, the manager of the person to whom it is assigned, personnel conducting an official audit) (IRS-defined)

10.8.26.3.1.12.3
(11-06-2023)
Access Control for Non-Government Furnished/Personally Owned (BYOD) Mobile Devices

                                                                      #
 #
 #
 #

(2) The IRS IT organization shall retain information system connection or processing agreements for approved non-government furnished/personally owned mobile devices that have been approved for use in the BYOD program. (IRS-defined)

10.8.26.3.2
(04-25-2022)
AT - Awareness and Training

(1) In addition to the Awareness and Training guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- AT-1 Awareness and Training Policy and Procedures
- AT-3 Role-Based Training
- AT-4 Training Records
- AT-5 Withdrawn by NIST
- AT-6 Training Feedback

10.8.26.3.2.1
(04-25-2022)
AT-2 Literacy Training and Awareness

(1) All supplemental policies required to implement mobile device security solutions shall be documented and provided to mobile device users. (IRS-defined)

(2) Mobile device users shall receive training on the following required topics before they are authorized to access an IRS network via a wireless remote access device: (IRS-defined)

    a.   User authentication and content encryption requirements.
    b.   Enabling wireless interfaces only when needed.
    c.   Enabling the VPN connection to the IRS network immediately after establishing a wireless connection (using an approved VPN client).
    d.   All Internet browsing being done on the IRS network, only after the VPN connection has been established.
    e.   Locations where wireless remote access is authorized or not authorized (e.g., home, airport, hotel, etc.).
    f.   Wireless client configuration requirements.
    g.   Use of Wi-Fi Protected Access 2 (WPA2) Personal (Advanced Encryption Standard (AES)) on home WLAN.

h.   Home WLAN password and Service Set Identifier (SSID) requirements - Discontinue the use of devices suspected of being tampered with and notify the site AO.

(3)   Refer to IRM 10.8.1 for additional guidance on Literacy Training and Awareness.

10.8.26.3.3 (04-25-2022) **AU - Audit and Accountability**	(1) In addition to the Audit and Accountability guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1: • AU-1 Audit and Accountability Policy and Procedures • AU-2 Event Logging • AU-6 Audit Review, Analysis, and Reporting • AU-7 Audit Reduction and Report Generation • AU-11 Audit Record Retention • AU-13 Monitoring for Information Disclosure • AU-15 Withdrawn by NIST • AU-16 Cross-Organizational Audit Logging

10.8.26.3.3.1
(04-25-2022)
AU-3 Content of Audit Records

(1)   The UEM server shall be configured to produce audit records containing information to establish what type of events occurred. (DISA UEM Server SRG: SRG-APP-000095-UEM-000055)

(2)   The UEM server shall be configured to produce audit records containing information to establish when (date and time) the events occurred. (DISA UEM server SRG: SRG-APP-000096-UEM-000056)

(3)   The UEM server shall be configured to produce audit records containing information to establish where the events occurred. (DISA UEM Server SRG: SRG-APP-000097-UEM-000057)

(4)   The UEM server shall be configured to produce audit records containing information to establish the source of the events. (DISA UEM Server SRG: SRG-APP-000098-UEM-000058)

(5)   The UEM server shall be configured to produce audit records that contain information to establish the outcome of the events. (DISA UEM Server SRG: SRG-APP-000099-UEM-000059)

(6)   The UEM server shall be configured to generate audit records containing information that establishes the identity of any individual or process associated with the event. (DISA UEM Server SRG: SRG-APP-000100-UEM-000060)

(7)   The UEM server shall be configured to generate audit records containing the full-text recording of privileged commands or the individual identities of group account users. (DISA UEM Server SRG: SRG-APP-000101-UEM-000061)

(8)   The UEM Agent shall record within each UEM Agent audit record the following information: (DISA UEM Agent SRG: SRG-APP-000097-UEM-100005)

a.   Date and time of the event,
b.   Type of event,
c.   Subject identity; and
d.   If relevant, the outcome (success or failure) of the event.

(9)   Refer to IRM 10.8.1 for additional guidance on Content of Audit Records.

10.8.26.3.3.2 (04-25-2022) **AU-4 Audit Log Storage Capacity**	(1) The UEM server shall be configured to transfer UEM server logs to another server for storage, analysis, and reporting. (DISA UEM Server SRG: SRG-APP-000358-UEM-000228) *Note:* UEM server logs include logs of UEM events and logs transferred to the UEM server by UEM agents of managed devices. (2) The UEM server shall, at a minimum, off-load audit logs of interconnected systems in real time and off-load standalone systems weekly. (DISA UEM Server SRG: SRG-APP-000515-UEM-000390) (3) The UEM Agent shall queue alerts if the trusted channel is not available. (DISA UEM Agent SRG: SRG-APP-000358-UEM-100003) (4) The UEM Agent shall be configured to enable the following function: transfer managed endpoint device audit logs read by the UEM Agent to an UEM server or third-party audit management server. (DISA UEM Agent SRG: SRG-APP-000358-UEM-100013) (5) Refer to IRM 10.8.1 for additional guidance on Audit Log Storage Capacity.
10.8.26.3.3.3 (04-25-2022) **AU-5 Response to Audit Logging Process Failures**	(1) The UEM SRG shall alert the ISSO and System Administrator (at a minimum) in the event of an audit processing failure. (DISA UEM Server SRG: SRG-APP-000108-UEM-000062) (2) Refer to IRM 10.8.1 for additional guidance on Response to Audit Logging Process Failures.
10.8.26.3.3.4 (04-25-2022) **AU-8 Time Stamps**	(1) The UEM server shall use host operating system clocks to generate time stamps for audit records. (DISA UEM Server SRG: SRG-APP-000116-UEM-000067) (2) The UEM server shall be configured to record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). (DISA UEM Server SRG: SRG-APP-000374-UEM-000244) (3) The UEM server shall be configured to record time stamps for audit records that meet a granularity for a minimum degree of precision, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000375-UEM-000245) (4) Refer to IRM 10.8.1 for additional guidance on Time Stamps.
10.8.26.3.3.5 (04-25-2022) **AU-9 Protection of Audit Information**	(1) The UEM server shall protect audit information from any type of unauthorized read access. (DISA UEM Server SRG: SRG-APP-000118-UEM-000068) (2) The UEM server shall protect audit information from unauthorized modification. (DISA UEM Server SRG: SRG-APP-000119-UEM-000069) (3) The UEM server shall protect audit information from unauthorized deletion. (DISA UEM Server SRG: SRG-APP-000120-UEM-000070) (4) The UEM server shall back up audit records, in accordance with IRM 10.8.1, onto a log management server. (DISA UEM Server SRG: SRG-APP-000125-UEM-000074)

(5)   Refer to IRM 10.8.1 for additional guidance on Protection of Audit Information.

10.8.26.3.3.6
(04-25-2022)
AU-10 Non-Repudiation

(1)   The UEM server shall protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation. (DISA UEM Server SRG: SRG-APP-000080-UEM-000044)

(2)   Refer to IRM 10.8.1 for additional guidance on Non-Repudiation.

10.8.26.3.3.7
(04-25-2022)
AU-12 Audit Record Generation

(1)   The UEM server shall provide audit record generation capability for IRS-defined auditable events within all application components. (DISA UEM Server SRG: SRG-APP-000089-UEM-000049)

(2)   The UEM server shall be configured to provide audit records in a manner suitable for the Authorized Administrators to interpret the information. (DISA UEM Server SRG: SRG-APP-000089-UEM-000050)

(3)   The UEM server shall be configured to allow only specific administrator roles to select which auditable events are to be audited. (DISA UEM Server SRG: SRG-APP-000090-UEM-000051)

(4)   The UEM server shall generate audit records when successful/unsuccessful attempts to access privileges occur. (DISA UEM Server SRG: SRG-APP-000091-UEM-000052)

(5)   The UEM server shall generate audit records when successful/unsuccessful attempts to access security objects occur. (DISA UEM Server SRG: SRG-APP-000492-UEM-000367)

(6)   The UEM server shall generate audit records when successful/unsuccessful attempts to modify privileges occur. (DISA UEM Server SRG: SRG-APP-000495-UEM-000370)

(7)   The UEM server shall generate audit records when successful/unsuccessful attempts to modify security objects occur. (DISA UEM Server SRG: SRG-APP-000496-UEM-000371)

(8)   The UEM server shall generate audit records when successful/unsuccessful attempts to delete privileges occur. (DISA UEM Server SRG: SRG-APP-000499-UEM-000374)

(9)   The UEM server shall generate audit records when successful/unsuccessful attempts to delete security objects occur. (DISA UEM Server SRG: SRG-APP-000501-UEM-000376)

(10)   The UEM server shall generate audit records when successful/unsuccessful logon attempts occur. (DISA UEM Server SRG: SRG-APP-000503-UEM-000378)

(11)   The UEM server shall generate audit records for privileged activities or other system-level access. (DISA UEM Server SRG: SRG-APP-000504-UEM-000379)

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Internal Revenue Manual

10.8.26.3.3.7

(12) The UEM server shall generate audit records showing starting and ending time for user access to the system. (DISA UEM Server SRG: SRG-APP-000505-UEM-000380)

(13) The UEM server shall generate audit records when concurrent logons from different workstations occur. (DISA UEM Server SRG: SRG-APP-000506-UEM-000381)

(14) The UEM server shall generate audit records when successful/unsuccessful accesses to objects occur. (DISA UEM Server SRG: SRG-APP-000507-UEM-000382)

(15) The UEM server shall generate audit records for all direct access to the information system. (DISA UEM Server SRG: SRG-APP-000508-UEM-000383)

(16) The UEM server shall generate audit records for all account creations, modifications, disabling, and termination events. (DISA UEM Server SRG: SRG-APP-000509-UEM-000384)

(17) The UEM Agent shall provide an alert via the trusted channel to the UEM Server in the event of any of the following audit events: (DISA UEM Agent SRG: SRG-APP-000089-UEM-100002)

    a. Successful application of policies to a mobile device,
    b. Receiving or generating periodic reachability events,
    c. Change in enrollment state,
    d. Failure to install an application from the UEM Server; and
    e. Failure to update an application from the UEM Server

(18) The UEM Agent shall generate a UEM Agent audit record of the following auditable events: (DISA UEM Agent SRG: SRG-APP-000089-UEM-100004)

    a. Startup and shutdown of the UEM Agent,
    b. UEM Policy update; and
    c. Any modification commanded by the UEM Server.

(19) The UEM Agent shall be configured to enable the following function: read audit logs of the managed endpoint device. (DISA UEM Agent SRG: SRG-APP-000089-UEM-100012)

(20) Refer to IRM 10.8.1 for additional guidance on Audit Record Generation.

10.8.26.3.3.8
(04-25-2022)
AU-14 Session Audit

(1) The UEM server shall initiate session auditing upon startup. (DISA UEM Server SRG: SRG-APP-000092-UEM-000053)

(2) Refer to IRM 10.8.1 for additional guidance on Session Audit.

10.8.26.3.4
(04-25-2022)
CA - Assessment, Authorization, and Monitoring

(1) In addition to the Assessment, Authorization, and Monitoring guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

    • CA-1 Assessment, Authorization, and Monitoring Policy and Procedures
    • CA-3 Information Exchange
    • CA-4 Withdrawn by NIST
    • CA-5 Plan of Action and Milestones (POA&M)
    • CA-6 Authorization

10.8.26.3.3.8   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
                                                                   Any line marked with a #
                                                                   is for **Official Use Only**

- CA-7 Continuous Monitoring
- CA-8 Penetration Testing

10.8.26.3.4.1
(04-25-2022)
CA-2 Control
Assessments

(1) Mobile devices that access, process, transmit, or store IRS information shall:

   a. Be documented in an Authorization package in accordance with IRM 10.8.1, TD-P 85-01, *Department of the Treasury IT Security Program*, and NIST Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems.* (IRS-defined)

      Note: Each individual mobile device does not need to have an Authorization for it; however, each mobile device configuration needs to go through the Authorization process and be documented in the package.

(2) Wireless devices connecting directly or indirectly (e.g., ActiveSync, wireless) to a network shall be included in the appropriate System's Authorization documentation (i.e., System Security Plan (SSP)). (IRS-defined)

(3) Mobile devices shall be approved by the AO prior to accessing IRS networks and data. (IRS-defined)

(4) Mobile devices that process SBU and PII are subject to a full security assessment prior to use. (IRS-defined)

   a. Cybersecurity Security Assessment Services (SAS) shall identify any security risk(s) and document the assessment of risk in a Security Assessment Report (SAR).

   b. The AO shall make a determination if the identified risk(s) are acceptable or not.

(5) Refer to IRM 10.8.1 for additional guidance on Assessments.

10.8.26.3.5
(04-25-2022)
CM - Configuration
Management

(1) In addition to the Configuration Management guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- CM-1 Configuration Management Policy and Procedures
- CM-3 Configuration Change Control
- CM-4 Impact Analysis
- CM-8 System Component Inventory
- CM-9 Configuration Management Plan
- CM-10 Software Usage Restrictions
- CM-12 Information Location
- CM-13 Data Action Mapping
- CM-14 Signed Components

10.8.26.3.5.1
(04-25-2022)
CM-2 Baseline
Configuration

(1) Configuration management procedures shall be developed for government furnished mobile devices in accordance with IRM 10.8.1 and this IRM. (IRS-defined)

(2) IRS developed configuration baselines for mobile device security shall be developed consistent with NIST 800-124 and NIST 800-37 when setting minimum security standards for mobile devices. (IRS-defined)

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Internal Revenue Manual

10.8.26.3.5.1

Note: The above guidance, including appropriate security controls specified in NIST SP 800-53, is in addition to all existing federal requirements for data protection and remote access for mobile devices.

(3) The IRS shall establish and maintain baseline configurations and inventories, including application software, throughout the respective System Development Life Cycle (SDLC) (i.e., IRS Enterprise Lifecycle (ELC)), of government furnished mobile devices that access, process, transmit, or store IRS information. (IRS-defined)

(4) Refer to IRM 10.8.1 for additional guidance on Baseline Configuration.

10.8.26.3.5.2
(04-25-2022)
CM-5 Access
Restrictions for Change

(1) The UEM server shall prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization. (DISA UEM Server SRG: SRG-APP-000131-UEM-000076)

(2) The UEM server shall limit privileges to change the software resident within software libraries. (DISA UEM Server SRG: SRG-APP-000133-UEM-000078)

(3) The UEM server shall enforce access restrictions associated with changes to the server configuration. (DISA UEM Server SRG: SRG-APP-000380-UEM-000251)

(4) The UEM server shall audit the enforcement actions used to restrict access associated with changes to the application. (DISA UEM Server SRG: SRG-APP-000381-UEM-000252)

(5) Refer to IRM 10.8.1 for additional guidance on Access Restrictions for Change.

10.8.26.3.5.3
(04-25-2022)
CM-6 Configuration
Settings

(1) Smart Card Readers (SCRs) used with government furnished mobile devices must have the IRS-approved software version installed. (IRS-defined)

(2) Government furnished and non-government furnished/personally owned mobile devices must be set to implement the security requirements within this IRM and IRM 10.8.1. (IRS-defined)

(3) Non-Government furnished/personally owned mobile devices that are enrolled in the BYOD program that are rooted or jailbroken must not be permitted. (IRS-defined)

    a.   Mobile device management servers must be configured to detect rooted or jailbroken devices.
    b.   IRS installed applications and/or software on detected rooted or jailbroken devices must be wiped.

      Note: Rooted and jailbroken are terms that describe the process of modifying the mobile device's operating system, often with the goal of running unsigned code or performing unsupported customizations to the operating system. Unlocking allows users to operate a mobile device on a cellular network it is not authorized to connect to.

10.8.26.3.5.2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

(4)   For guidance on operating system-specific configuration settings, see the Mobile Device Technical Security Requirements Exhibits within this IRM

(5)   The UEM server shall be configured in accordance with the security configuration settings based on IRS security configuration or implementation guidance, including STIGs. (DISA UEM Server SRG: SRG-APP-000516-UEM-000391)

(6)   The UEM server shall be configured to allow authorized administrators to read all audit data from audit records on the server. (DISA UEM Server SRG: SRG-APP-000516-UEM-000392)

(7)   The UEM Agent shall record the reference identifier of the UEM Server during the enrollment process. (DISA UEM Agent SRG: SRG-APP-000516-UEM-100006)

(8)   The UEM Agent shall perform the following functions: (DISA UEM Agent SRG: SRG-APP-000516-UEM-100010)

   a.   Enroll in management,
   b.   Configure whether users can unenroll from management; and
   c.   Configure periodicity of reachability events.

(9)   The UEM Agent shall be configured to perform one of the following actions upon an attempt to unenroll the mobile device from management: (DISA UEM Agent SRG: SRG-APP-000516-UEM-100011)

   a.   Prevent the unenrollment from occurring,
   b.   Wipe the device to factory default settings; and
   c.   Wipe the work profile with all associated applications and data.

(10) Refer to IRM 10.8.1 for additional guidance on Configuration Settings.

10.8.26.3.5.4
(04-25-2022)
CM-7 Least Functionality

(1)   The UEM server shall be configured to disable non-essential capabilities. (DISA UEM Server SRG: SRG-APP-000141-UEM-000079)

(2)   The firewall protecting the UEM server platform shall be configured so only ports, protocols, and services approved by User and Network Services (UNS) and Computer Security Incident Response Center (CSIRC) are enabled. (DISA UEM Server SRG: SRG-APP-000142-UEM-000080)

(3)   The UEM server shall be configured to use only documented platform APIs. (DISA UEM Server SRG: SRG-APP-000142-UEM-000081)

(4)   The UEM server shall disable functions, ports, protocols, and services (within the application) deemed unnecessary and/or non-secure, in accordance with UNS and CSIRC. (DISA UEM Server SRG: SRG-APP-000383-UEM-000254)

(5)   Refer to IRM 10.8.1 for additional guidance on Least Functionality.

10.8.26.3.5.5
(04-25-2022)
CM-11 User-Installed Software

(1)   The UEM server shall verify the digital signature of software before installation and alert the ISSO and other designated personnel if unauthorized software is detected. (DISA UEM Server SRG: SRG-APP-000377-UEM-000247)

(2)   The UEM server shall prohibit user installation of software by an administrator without the appropriate assigned permission for software installation. (DISA UEM Server SRG: SRG-APP-000378-UEM-000248)

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.5.5**
Any line marked with a #
is for **Official Use Only**

(3) The UEM server shall be configured to only allow enrolled devices that are compliant with UEM policies and assigned to a user in the application access group to download applications. (DISA UEM Server SRG: SRG-APP-000378-UEM-000249)

(4) Refer to IRM 10.8.1. for additional guidance on User-Installed Software.

10.8.26.3.6
(04-25-2022)
CP - Contingency
Planning

(1) Refer to IRM 10.8.1 for guidance on Contingency Planning.

10.8.26.3.7
(04-25-2022)
IA - Identification and
Authentication

(1) In addition to the Identification and Authentication guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- IA-1 Identification and Authentication Policy and Procedures
- IA-8 Identification and Authentication (Non-Organizational Users)
- IA-9 Service Identification and Authentication
- IA-10 Adaptive Authentication
- IA-12 Identity Proofing

10.8.26.3.7.1
(04-25-2022)
IA-2 Identification and
Authentication
(Organizational Users)

(1) The UEM server shall uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users). (DISA UEM Server SRG: SRG-APP-000148-UEM-000082)

(2) The UEM server shall be configured to use an IRS Central Directory Service to provide multifactor authentication for network access to privileged and non-privileged accounts. (DISA UEM Server SRG: SRG-APP-000149-UEM-000083)

(3) All UEM server local accounts created during application installation and configuration shall be removed. (DISA UEM Server SRG: SRG-APP-000151-UEM-000085)

Note: In this context local accounts refers to user and or administrator accounts on the server that use user name and password for user access and authentication.

(4) The UEM server shall ensure users are authenticated with an individual authenticator prior to using a group authenticator. (DISA UEM Server SRG: SRG-APP-000153-UEM-000087)

(5) The UEM server shall be configured to use IRS PKI for multifactor authentication. This requirement is included in SRG-APP-000149. (DISA UEM Server SRG: SRG-APP-000154-UEM-000088)

(6) The UEM server shall use FIPS-validated Secure Hash Algorithm 2 (SHA-2) or higher hash function to provide replay-resistant authentication mechanisms for network access to privileged accounts. (DISA UEM Server SRG: SRG-APP-000156-UEM-000090)

(7) The UEM server shall implement replay-resistant authentication mechanisms for network access to non-privileged accounts. (DISA UEM Server SRG: SRG-APP-000157-UEM-000091)

10.8.26.3.6   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
                                                                    Any line marked with a #
                                                                    is for **Official Use Only**

(8) Refer to IRM 10.8.1 for additional guidance on Identification and Authentication (Organizational Users).

10.8.26.3.7.2
(04-25-2022)
IA-3 Device Identification and Authentication

(1) Before establishing a connection to any endpoint device being managed, the UEM server shall establish a trusted path between the server and endpoint that provides assured identification of the end point using a bidirectional authentication mechanism configured with a FIPS-validated AES cipher block algorithm to authenticate with the device. (DISA UEM Server SRG: SRG-APP-000395-UEM-000266)

(2) The UEM server shall authenticate endpoint devices (servers) before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based. (DISA UEM Server SRG: SRG-APP-000580-UEM-000398)

(3) If cipher suites using pre-shared keys are used for device authentication, the UEM server shall have a minimum-security strength of 112 bits or higher. (DISA UEM Server SRG: SRG-APP-000585-UEM-000399)

(4) Refer to IRM 10.8.1 for additional guidance on Device Identification and Authentication.

10.8.26.3.7.3
(04-25-2022)
IA-4 Identifier Management

(1) The UEM server shall disable identifiers (individuals, groups, roles, and devices) after a period of inactivity, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000163-UEM-000093)

(2) Refer to IRM 10.8.1 for additional guidance on Identifier Management.

10.8.26.3.7.4
(04-25-2022)
IA-5 Authenticator Management

(1) Authentication when accessing IRS systems and data (e.g., email, files) via mobile devices (BYOD or IRS-owned) shall be in accordance with IRM 10.8.1 and HSPD-12. (IRS-Defined)

(2) Passwords/passcodes shall be created and maintained in accordance with IRM 10.8.1 and the appropriate underlying OS security requirements checklist where applicable. (IRS-defined)

(3) A password shall be enabled for each wireless client that connects to an IRS network or system. Passwords shall comply with IRM 10.8.1. (IRS-defined)

(4) Government furnished mobile device users shall be prevented from changing the user profile on their assigned mobile devices. (IRS-defined)

(5) The UEM server shall enforce a minimum password length, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000164-UEM-000094)

(6) The UEM server shall prohibit password reuse for a minimum number of generations, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000165-UEM-000095)

(7) The UEM server shall:

  a. Enforce password complexity by requiring that at least one uppercase character be used. (DISA UEM Server SRG: SRG-APP-000166-UEM-000096)

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Internal Revenue Manual

10.8.26.3.7.4

      b.   Enforce password complexity by requiring that at least one lowercase character be used. (DISA UEM Server SRG: SRG-APP-000167-UEM-000097)

      c.   Enforce password complexity by requiring that at least one numeric character be used. (DISA UEM Server SRG: SRG-APP-000168-UEM-000098)

      d.   Enforce password complexity by requiring that at least one special character be used. (DISA UEM Server SRG: SRG-APP-000169-UEM-000099)

(8)   The UEM server shall require the change of a number of characters, in accordance with IRM 10.8.1, when passwords are changed. (DISA UEM Server SRG: SRG-APP-000170-UEM-000100)

(9)   For UEM server using password authentication, the application shall store only cryptographic representations of passwords. (DISA UEM Server SRG: SRG-APP-000171-UEM-000101)

(10)   For UEM server using password authentication, the network element shall use FIPS-validated SHA-2 or later protocol to protect the integrity of the password authentication process. (DISA UEM Server SRG: SRG-APP-000172-UEM-000102)

(11)   The UEM server shall enforce 24 hours/1 day as the minimum password lifetime. (DISA UEM Server SRG: SRG-APP-000173-UEM-000103)

(12)   The UEM server shall enforce a maximum password lifetime restriction, in accordance with IRM 10.8.1. (DISA UEM Server SRG: SRG-APP-000174-UEM-000104)

(13)   When using PKI-based authentication for user access, the UEM server shall validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor. (DISA UEM Server SRG: SRG-APP-000175-UEM-000105)

(14)   When the UEM server cannot establish a connection to determine the validity of a certificate, the server shall be configured not to have the option to accept the certificate. (DISA UEM Server SRG: SRG-APP-000175-UEM-000106)

(15)   The UEM server, when using PKI-based authentication, shall enforce authorized access to the corresponding private key. (DISA UEM Server SRG: SRG-APP-000176-UEM-000107)

(16)   The UEM server shall map the authenticated identity to the individual user or group account for PKI-based authentication. (DISA UEM Server SRG: SRG-APP-000177-UEM-000108)

(17)   The UEM server shall prohibit the use of cached authenticators after an organization-defined time period. (DISA UEM Server SRG: SRG-APP-000400-UEM-000271)

(18)   The UEM server, for PKI-based authentication, shall implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network. (DISA UEM Server SRG: SRG-APP-000401-UEM-000272)

(19) The UEM server shall validate certificates used for TLS functions by performing RFC 5280-compliant certification path validation. (DISA UEM Server SRG: SRG-APP-000605-UEM-000401)

(20) The UEM Agent shall not install policies if the policy-signing certificate is deemed invalid. (DISA UEM Agent SRG: SRG-APP-000175-UEM-100008)

(21) The UEM Agent shall use managed endpoint device key storage for all persistent secret and private keys. (DISA UEM Agent SRG: SRG-APP-000176-UEM-100001)

(22) Refer to IRM 10.8.1 for additional guidance on Authenticator Management.

10.8.26.3.7.5
(04-25-2022)
IA-6 Authentication Feedback

(1) The UEM server shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. (DISA UEM Server SRG: SRG-APP-000178-UEM-000109)

(2) Refer to IRM 10.8.1 for additional guidance on Authentication Feedback.

10.8.26.3.7.6
(04-25-2022)
IA-7 Cryptographic Module Authentication

(1) The UEM server shall use FIPS-validated SHA-2 or higher hash function to protect the integrity of keyed-hash message authentication code (HMAC), Key Derivation Functions (KDFs), Random Bit Generation, and hash-only applications. (DISA UEM Server SRG: SRG-APP-000179-UEM-000110)

(2) The application shall use FIPS-validated SHA-256 or higher hash function for digital signature generation and verification. (DISA UEM Server SRG: SRG-APP-000610-UEM-000402)

(3) Refer to IRM 10.8.1 for additional guidance on Cryptographic Module Authentication.

10.8.26.3.7.7
(04-25-2022)
IA-11 Re-Authentication

(1) The UEM server shall require users (administrators) to reauthenticate when roles change. (DISA UEM Server SRG: SRG-APP-000389-UEM-000260)

(2) The UEM server shall require end-point devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication. Examples include: (DISA UEM Server SRG: SRG-APP-000390-UEM-000261)

    a.   After a screen lock,
    b.   After device reboot,
    c.   Before installation of new device policy or profile; and
    d.   Before executing a device reset or wipe.

(3) Refer to IRM 10.8.1 for additional guidance on Re-Authentication.

10.8.26.3.8
(04-25-2022)
IR - Incident Response

(1) In addition to the Incident Response guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- Incident Response Policy and Procedures
- IR-2 Incident Response Training
- IR-3 Incident Response Testing
- IR-4 Incident Handling
- IR-5 Incident Monitoring
- IR-7 Incident Response Assistance

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.8**
Any line marked with a #
is for **Official Use Only**

- IR-8 Incident Response Plan
- IR-9 Information Spillage Response
- IR-10 Withdrawn by NIST

10.8.26.3.8.1
(04-25-2022)
IR-6 - Incident Reporting

(1) Employees shall cooperate with CSIRC during the investigation of any incidents reported by them. (TD P 85-01 Vol. I, Section 2.15)

(2) Refer to the following resources for additional incident reporting requirements not addressed within this IRM (Departmental Incident Response Plan):

    a. IRM 10.2.8, *Physical Security Program, Incident Reporting*.

                                                                                                      #
                                                                                                    #

(3) Refer to IRM 10.8.1 for additional guidance on Incident Reporting.

10.8.26.3.9
(04-25-2022)
MA - Maintenance

(1) In addition to the Maintenance guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- MA-1 Maintenance Policy and Procedures
- MA-2 Controlled Maintenance
- MA-3 Maintenance Tools
- MA-5 Maintenance Personnel
- MA-6 Timely Maintenance
- MA-7 Field Maintenance

10.8.26.3.9.1
(04-25-2022)
MA-4 Non-Local Maintenance

(1) The UEM server shall configure web management tools with FIPS-validated AES cipher block algorithm to protect the confidentiality of maintenance and diagnostic communications for nonlocal maintenance sessions. (DISA UEM Server SRG: SRG-APP-000412-UEM-000283)

(2) The UEM server shall verify remote disconnection when non-local maintenance and diagnostic sessions are terminated. (DISA UEM Server SRG: SRG-APP-000413-UEM-000284)

(3) Refer to IRM 10.8.1 for additional guidance on Non-Local Maintenance.

10.8.26.3.10
(04-25-2022)
MP - Media Protection

(1) In addition to the Media Protection guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- MP-1 Media Protection Policy and Procedures
- MP-2 Media Access
- MP-3 Media Marking
- MP-4 Media Storage
- MP-5 Media Transport
- MP-8 Media Downgrading

10.8.26.3.10.1
(11-06-2023)
MP-6 Media Sanitization

(1) The IRS IT organization shall develop procedures for the sanitization and disposal of government furnished mobile devices. (IRS-defined)

    a. Procedures shall be followed to ensure that all IRS mobile devices that have processed sensitive information are disposed of.
    b. Government furnished mobile devices shall be cleansed by utilizing commercial disk-wiping software.

10.8.26.3.8.1   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

(2)   The IRS IT organization shall keep an inventory of all disposed government furnished mobile devices. (IRS-defined)

(3)   The IRS IT organization shall develop procedures for the sanitization of non-government furnished/personally owned mobile devices. (IRS-defined)

\#
\#
\#
\#
\#
\#

\#
\#
\#
\#

(5)   All mobile devices shall follow the device manufacturer's instructions for wiping user data installed from the device memory and the media card. (IRS-defined)

(6)   Refer to IRM 10.8.1 for additional guidance on Media Sanitization.

10.8.26.3.10.2
(04-25-2022)
MP-7 Media Use

(1)   Government furnished mobile devices with removable memory cards (e.g., MicroSD) shall abide by the following requirements: (IRS-defined)

   a.   Data stored on the card shall be encrypted with a FIPS 140-validated encryption technology solution.
   b.   The card shall be bound to the mobile device such that it cannot be read by any other mobile device or computer.

(2)   BYOD participants shall not store any IRS data on a removable memory card. (IRS-defined)

(3)   Refer to IRM 10.8.1 for additional guidance on Media Use.

10.8.26.3.11
(04-25-2022)
PE - Physical and Environmental Protection

(1)   In addition to the Physical and Environmental Protection guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

   •   PE-1 Physical and Environmental Protection Policy and Procedures
   •   PE-2 Physical Access Authorizations
   •   PE-4 Access Control for Transmission Medium
   •   PE-5 Access Control for Output Devices
   •   PE-6 Monitoring Physical Access
   •   PE-7 Withdrawn by NIST
   •   PE-8 Visitor Access Records
   •   PE-9 Power Equipment and Cabling
   •   PE-10 Emergency Shutoff
   •   PE-11 Emergency Power
   •   PE-12 Emergency Lighting
   •   PE-13 Fire Protection
   •   PE-14 Environmental Controls
   •   PE-15 Water Damage Protection
   •   PE-16 Delivery and Removal
   •   PE-17 Alternate Work Site

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.11**
Any line marked with a #
is for **Official Use Only**

- PE-18 Location of System Components
- PE-19 Information Leakage
- PE-20 Asset Monitoring and Tracking
- PE-21 Electromagnetic Pulse Protection
- PE-22 Component Marking
- PE-23 Facility Location

10.8.26.3.11.1
(04-25-2022)
PE-3 Physical Access Control

(1) At all times, government furnished and non-government furnished/personally owned mobile device users shall: (IRS-defined)

    a. Be responsible for the physical security of their mobile device(s).
    b. Secure their mobile device(s) when not in their possession.
    c. Never leave their powered-on mobile device unlocked when it is not in their presence.
    d. Secure their mobile device(s) (e.g., cable lock, screen lock) from theft or tampering when located in an IRS facility and at an approved telework location (e.g., home).
    e. When traveling; if additional screening is required during the airport screening process, inform the security agent that you cannot be separated from your government furnished mobile device (e.g., laptop) at any time, and that it shall be kept in your possession.

(2) The IRS Physical Security organization shall develop and implement procedures for physical mobile device security compliance. (IRS-defined)

(3) Passwords/passcodes, hardware tokens, and/or smart cards shall not be stored on/or with a mobile device or laptop, unless encrypted or otherwise under the direct and continuous control of the authorized user. (IRS-defined)

(4) Mobile devices with wireless capability (e.g. smart phones, peripheral devices) shall be restricted from any area where classified IRS systems process information or where classified information is discussed. (IRS-defined)

(5) Refer to IRM 10.8.1, the IRM 10.2.x, *Physical Security Program* series of IRMs, and IRM 1.4.6, *Managers Security Handbook* for additional physical and environmental protection security guidance.

10.8.26.3.12
(04-25-2022)
PL – Planning

(1) In addition to the Security Planning guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- PL-1 Planning Policy and Procedure
- PL-2 System Security and Privacy Plans
- PL-3 Withdrawn by NIST
- PL-5 Withdrawn by NIST
- PL-6 Withdrawn by NIST
- PL-7 Concept of Operations
- PL-8 Security and Privacy Architectures
- PL-9 Central Management
- PL-10 Baseline Selection
- PL-Baseline Tailoring

10.8.26.3.12.1
(04-25-2022)
PL-4 Rules of Behavior

(1) In addition to the Rules of Behavior requirements within this IRM, the Rules of Behavior requirements defined in IRM 10.8.1 shall be implemented.

10.8.26.3.12.1.1
(11-06-2023)
Rules of Behavior for BYOD Participants

(1) In order to connect a non-government furnished/personally owned mobile device to the IRS network with the capability of backing up, storing, or otherwise accessing IRS data of any type, BYOD participants shall: (IRS-defined)

    a.   Understand and acknowledge that they shall comply with all rules and procedures made applicable to its use.
    b.   Be responsible for the physical security of their mobile device.
    c.   Be responsible for backing up their personal data.
    d.   Understand that mobile devices which are not in compliance with IRS security policies or represent any unacceptable risk to the IRS network or data will not be allowed to connect to the IRS systems.

  #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #
 #

(2) The IRS reserves the right to disconnect any non-government furnished/personally owned mobile device from IRS system resources if the mobile device is used in a way that puts IRS systems or data, or the data of taxpayers or other persons, at an unacceptable risk of harm or disclosure. (IRS-defined)

(3) The Government will not be liable for damages to any personal property that may occur during the course of performing IRS-related duties, except to the extent that the Government is held liable under the Federal Tort Claims Act or the Military Personnel and Civilian Employee's Claims Act.(IRS-defined)

10.8.26.3.13
(04-25-2022)
PM - Program Management

(1) Refer to IRM 10.8.1 for guidance on Program Management.

10.8.26.3.14
(04-25-2022)
PS - Personnel Security

(1) Refer to IRM 10.8.1 for guidance on Personnel Security.

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Internal Revenue Manual

10.8.26.3.14

10.8.26.3.15
(04-25-2022)
PT - Personally Identifiable Information Processing and Transparency

(1) Refer to IRM 10.8.1 for guidance on Personally Identifiable Information Processing and Transparency

10.8.26.3.16
(04-25-2022)
RA - Risk Assessment

(1) In addition to the Risk Assessment guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- RA-1 Risk Assessment Policy and Procedures
- RA-2 Security Categorization
- RA-4 Withdrawn by NIST
- RA-5 Vulnerability Monitoring and Scanning
- RA-6 Technical Surveillance Countermeasures Survey
- RA-7 Risk Response
- RA-8 Privacy Impact Assessments
- RA-9 Criticality Analysis
- RA-10 Threat Hunting

10.8.26.3.16.1
(04-25-2022)
RA-3 Risk Assessment

(1) Risk assessments of mobile devices shall adhere to the requirements and be conducted using this manual, IRM 10.8.1 , the security checklists pertaining to this IRM, as well those of other pertinent IRMs (e.g., operating system, wireless). (IRS-defined)

   a. Any deficiencies in compliance shall be documented in a risk assessment report and brought to the attention of the responsible AO.

(2) Government furnished mobile devices with wireless capabilities shall have the additional risks and mitigations associated with non-government facilities, identified in a risk assessment. (IRS-defined)

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

10.8.26.3.17
(04-25-2022)
SA - System and Services Acquisition

(1) In addition to the System and Services Acquisition guidance defined within this IRM, controls shall be implemented in accordance with IRM 10.8.1:

- SA-1 System and Services Acquisition Policy and Procedures
- SA-2 Allocation of Resources
- SA-4 Acquisition Process
- SA-5 Information System Documentation
- SA-6 Withdrawn by NIST
- SA-7 Withdrawn by NIST
- SA-8 Security and Privacy Engineering Principles
- SA-9 External System Services
- SA-10 Developer Configuration Management
- SA-11 Developer Testing and Evaluation
- SA-12 Withdrawn by NIST
- SA-13 Withdrawn by NIST
- SA-14 Withdrawn by NIST
- SA-15 Development Process, Standards, and Tools
- SA-16 Developer-Provided Training
- SA-17 Develop Security and Privacy Architecture and Design
- SA-18 Withdrawn by NIST

10.8.26.3.15   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

- SA-19 Withdrawn by NIST
- SA-20 Customized Development of Critical Components
- SA-21 Developer Screening
- SA-22 Unsupported System Components
- SA-23 Specialization

10.8.26.3.17.1 (04-25-2022) **SA-3 System Development Life Cycle (SDLC)**	(1)	Wireless devices shall adhere to the IRS ELC in accordance with IRM 10.8.1. (IRS-defined)
	(2)	Refer to IRM 10.8.1 for additional guidance on System Development Life Cycle (SDLC).
10.8.26.3.17.2 (04-25-2022) **SA-4 Acquisition Process**	(1)	Wireless products shall be acquired, accounted for, and inventoried in accordance with IRM 10.8.1. (IRS-defined)
	(2)	Refer to IRM 10.8.1 for additional guidance on Acquisition Process.
10.8.26.3.18 (04-25-2022) **SC - System and Communications Protection**	(1)	In addition to the System and Communications Protection guidance defined within this IRM, controls shall be implemented in accordance with IRM 10.8.1:

- SC-1 System and Communications Protection Policy and Procedures
- SC-2 Separation of System and User Functionality
- SC-3 Security Function Isolation
- SC-4 Information in Shared System Resources
- SC-5 Denial of Service Protection
- SC-6 Resource Availability
- SC-7 Boundary Protection
- SC-9 Withdrawn by NIST
- SC-10 Network Disconnect
- SC-11 Trusted Path
- SC-12 Cryptographic Key Establishment and Management
- SC-14 Withdrawn by NIST
- SC-15 Collaborative Computing Devices and Applications
- SC-16 Transmission of Security and Privacy Attributes
- SC-17 Public Key Infrastructure (PKI) Certificates
- SC-18 Mobile Code
- SC-19 Withdrawn by NIST
- SC-20 Secure Name /Address Resolution Service (Authoritative Source)
- SC-21 Secure Name /Address Resolution Service (Recursive or Caching Resolver)
- SC-22 Architecture and Provisioning for Name/Address Resolution Service
- SC-25 Thin Nodes
- SC-26 Decoys
- SC-27 Platform-Independent Applications
- SC-28 Protection of Information at Rest
- SC-29 Heterogeneity
- SC-30 Concealment and Misdirection
- SC-31 Covert Channel Analysis
- SC-32 System Partitioning
- SC-33 Withdrawn by NIST
- SC-34 Non-Modifiable Executable Programs
- SC-35 External Malicious Code Identification
- SC-36 Distributed Processing and Storage

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.18**
Any line marked with a #
is for **Official Use Only**

- SC-37 Out-of-Band Channels
- SC-38 Operations Security
- SC-39 Process Isolation
- SC-40 Wireless Link Protection
- SC-41 Port and I/O Device Access
- SC-42 Sensor Capability and Data
- SC-43 Usage Restrictions
- SC-44 Detonation Chambers
- SC-45 System Time Synchronization
- SC-46 Cross Domain Policy Enforcement
- SC-47 Alternate Communications Paths
- SC-48 Sensor Relocation
- SC-49 Hardware-Enforced Separation and Policy Enforcement
- SC-50 Software-Enforced Separation and Policy Enforcement
- SC-51 Hardware-Based Protection

10.8.26.3.18.1
(11-06-2023)
SC-8 Transmission
Confidentiality and
Integrity

(2) The UEM server shall connect to IRS approved applications and managed mobile devices with an authenticated and secure (encrypted) connection to protect the confidentiality and integrity of transmitted information. (DISA UEM Server SRG: SRG-APP-000439-UEM-000313)

(3) Refer to IRM 10.8.1 for additional guidance on Transmission Confidentiality and Integrity.

10.8.26.3.18.2
(04-25-2022)
SC-11 Trusted Path

(1) The UEM server shall be configured to provide a trusted communication channel between itself and authorized IT entities using: (DISA UEM Server SRG: SRG-APP-000191-UEM-000117)

   a. Internet Protocol Security (IPsec),
   b. Secure Shell Protocol (SSH),
   c. Mutually authenticated TLS,
   d. Mutually authenticated Datagram Transport Layer Security (DTLS); and/or
   e. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

(2) The UEM server shall be configured to invoke either host-OS functionality or server functionality to provide a trusted communication channel between itself and remote administrators that provides assured identification of its endpoints and protection of the communicated data from modification and disclosure using: (DISA UEM Server SRG: SRG-APP-000191-UEM-000118)

   a. IPsec,
   b. SSH,
   c. TLS; and/or
   d. HTTPS

(3) The UEM server shall be configured to invoke either host-OS functionality or server functionality to provide a trusted communication channel between itself and managed devices that provides assured identification of its endpoints and

protection of the communicated data from modification and disclosure using: (DISA UEM Server SRG: SRG-APP-000191-UEM-000119)

    a.   TLS

    b.   HTTPS

(4)   Refer to IRM 10.8.1 for additional guidance on Trusted Path.

10.8.26.3.18.3
(04-25-2022)
SC-13 Cryptographic Protection

(1)   Data exchange shall be encrypted in accordance with the encryption standards of this IRM and IRM 10.8.1. (IRS-defined)

(2)   The UEM server shall use a FIPS-validated cryptographic module to generate cryptographic hashes. (DISA UEM Server SRG: SRG-APP-000514-UEM-000389)

(3)   The UEM server shall be configured to implement FIPS 140-validated mode for all server and agent encryption. (DISA UEM Server SRG: SRG-APP-000555-UEM-000393)

(4)   All UEM Agent cryptography supporting IRS functionality shall be FIPS 140-validated. (DISA UEM Agent SRG: SRG-APP-000555-UEM-100014)

(5)   Refer to IRM 10.8.1 for additional guidance on Cryptographic Protection.

10.8.26.3.18.3.1
(11-01-2021)

                     #
 #
 #
 #
 #

 #
 #
 #
 #

 #
 #

 #
 #

 #
 #
 #

 #
 #
 #
 #
 #
 #

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.18.3.1**
Any line marked with a #
is for **Official Use Only**

10.8.26.3.18.3.2   #
(11-01-2021)   #
                                                                                   #
                                                                                   #

                                                                                   #
                                                                                   #

                                                                                   #
                                                                                   #
                                                                                   #

                                                                                   #
                                                                                   #

10.8.26.3.18.3.3   (1) The IRS has made a decision to allow the use of taxpayer address information
(07-21-2020)   on Global Positioning System (GPS) devices. The Office of Privacy, Govern-
Global Positioning   mental Liaison and Disclosure (PGLD), has published specific guidelines for
System (GPS) Devices   use of Taxpayer address data on personally-owned GPS devices. See IRM
                        10.5.1.6.11, *Global Positioning Systems (GPS).* (IRS-defined)

                    (2) Users of GPS devices should be advised that many GPS devices, such as
                         those installed in smartphones and some automobiles, use telematics to
                         transmit address information entered by the user to the GPS vendor.
                         Therefore, IRS personnel shall:

                         a.   Only enter Taxpayer address information into the GPS. No other
                              Taxpayer-identifiable information shall be entered into GPS devices. (IRS-
                              defined)
                         b.   Immediately delete all Taxpayer address information from the GPS device
                              upon arrival at the destination address. (IRS-defined)

                    (3) If the GPS device requires a corresponding name or identifier for the address,
                         use a made-up number or other moniker that does not include any Taxpayer
                         PII or IRS-related information. (IRS-defined)

                    (4) IRS-owned or personally owned GPS devices shall not be connected to an
                         IRS computer.

                         a.   The ACIO Cybersecurity has made a Risk-Based Decision to allow the
                              connection of IRS-procured GPS devices to personally owned computers
                              for the purpose of updating map information and firmware. (IRS-defined)

10.8.26.3.18.4   (1) The UEM server shall protect the authenticity of communications sessions.
(04-25-2022)   (DISA UEM Server SRG: SRG-APP-000219-UEM-000132)
SC-23 Session
Authenticity   (2) The UEM server shall invalidate session identifiers upon user logout or other
                         session termination. (DISA UEM Server SRG: SRG-APP-000220-UEM-000133)

                    (3) The UEM server shall recognize only system-generated session identifiers.
                         (DISA UEM Server SRG: SRG-APP-000223-UEM-000134)

10.8.26.3.18.3.2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
                                                          Any line marked with a #
                                                              is for **Official Use Only**

(4)   The UEM server shall generate unique session identifiers using a FIPS-validated Random Number Generator (RNG) based on the Deterministic Random Bit Generators (DRBG) algorithm. (DISA UEM Server SRG: SRG-APP-000224-UEM-000135)

(5)   The UEM server shall only allow the use of IRS PKI established certificate authorities for verification of the establishment of protected sessions. (DISA UEM Server SRG: SRG-APP-000427-UEM-000298)

(6)   The UEM server shall be configured to use X.509v3 certificates for code signing for system software updates. (DISA UEM Server SRG: SRG-APP-000427-UEM-000299)

(7)   The UEM server shall be configured to use X.509v3 certificates for code signing for integrity verification. (DISA UEM Server SRG: SRG-APP-000427-UEM-000300)

(8)   The UEM Agent shall only accept policies and policy updates that are digitally signed by a certificate that has been authorized for policy updates by the UEM Server. (DISA UEM Agent SRG: SRG-APP-000427-UEM-100007)

(9)   The UEM Agent shall perform the following functions: Import the certificates to be used for authentication of UEM Agent communications. (DISA UEM Agent SRG: SRG-APP-000427-UEM-100009)

(10) Refer to IRM 10.8.1 for additional information on Session Authenticity.

10.8.26.3.18.5
(04-25-2022)
SC-24 Fail in Known State

(1)   The UEM server shall fail to a secure state if system initialization fails, shutdown fails, or aborts fail. (DISA UEM Server SRG: SRG-APP-000225-UEM-000136)

(2)   In the event of a system failure, the UEM server shall preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes. (DISA UEM Server SRG: SRG-APP-000226-UEM-000137)

(3)   Refer to IRM 10.8.1 for additional information on Fail in a Known State.

10.8.26.3.19
(04-25-2022)
SI - System and Information Integrity

(1)   In addition to the System and Information Integrity guidance defined within this IRM, the following controls shall be implemented in accordance with IRM 10.8.1:

- SI-1 System and Information Integrity Policy and Procedures
- SI-3 Malicious Code Protection
- SI-4 System Monitoring
- SI-5 Security Alerts, Advisories, and Directives
- SI-8 Spam Protection
- SI-9 Withdrawn by NIST
- SI-12 Information Management and Retention
- SI-14 Non-Persistence
- SI-15 Information Output Filtering
- SI-16 Memory Protection
- SI-17 Fail-Safe Procedures
- SI-18 Personally Identifiable Information Quality Operations
- SI-19 De-Identification
- SI-20 Tainting

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.19**
Any line marked with a #
is for **Official Use Only**

- SI-21 Information Refresh
- SI-22 Information Diversity
- SI-23 Information Fragmentation

10.8.26.3.19.1
(04-25-2022)
SI-2 Flaw Remediation

(1) Wireless application servers shall have the latest virus scanning and security patches installed and updated to detect and prevent viruses and other malicious content from infecting the enterprise network, in accordance with IRM 10.8.1 and IRM 10.8.54, *Minimum Firewall Administration Requirements*. (SI-2(2)_T.235)

(2) Per IRM 10.8.50, Security firmware updates and patches to government furnished mobile device hardware and software components shall be fully tested prior to deployment. (IRS-defined)

(3) The UEM server shall remove old software components after updated versions have been installed. (DISA UEM Server SRG: SRG-APP-000454-UEM-000328)

(4) The UEM server shall be maintained at a supported version. (DISA UEM Server SRG: SRG-APP-000456-UEM-000330)

(5) Refer to IRM 10.8.1 for additional guidance on Flaw Remediation.

10.8.26.3.19.2
(04-25-2022)
SI-6 Security and Privacy Function Verification

(1) The application shall notify the ISSO of failed security verification tests. (DISA UEM Server SRG: SRG-APP-000275-UEM-000157)

(2) The UEM server shall be configured with the periodicity of the following commands to the agent, in accordance with IRM 10.8.1: - query connectivity status - query the current version of the managed device firmware/software - query the current version of installed mobile applications - read audit logs kept by the managed device. (DISA UEM Server SRG: SRG-APP-000472-UEM-000347)

(3) The UEM server shall run a suite of self-tests during initial start-up (power on) to demonstrate correct operation of the server. (DISA UEM Server SRG: SRG-APP-000473-UEM-000348)

(4) The UEM server shall alert the system administrator when anomalies in the operation of security functions are discovered. (DISA UEM Server SRG: SRG-APP-000474-UEM-000349)

(5) Refer to IRM 10.8.1 for additional guidance on Security and Privacy Function Verification.

10.8.26.3.19.3
(04-25-2022)
SI-7 Software, Firmware, and Information Integrity

(1) The UEM server shall be configured to verify software updates to the server using a digital signature mechanism prior to installing those updates. (DISA UEM Server SRG: SRG-APP-000479-UEM-000354)

(2) Refer to IRM 10.8.1 for additional guidance on Software, Firmware, and Information Integrity.

10.8.26.3.19.4
(04-25-2022)
SI-10 Information Input Validation

(1) The UEM server shall check the validity of all data inputs. (DISA UEM Server SRG: SRG-APP-000251-UEM-000148)

10.8.26.3.19.1   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

(2)   The UEM server shall be configured to write to the server event log when invalid inputs are received. (DISA UEM Server SRG: SRG-APP-000447-UEM-000321)

(3)   Refer to IRM 10.8.1 for additional guidance on Information Input Validation.

10.8.26.3.19.5
(04-25-2022)
SI-11 Error Handling

(1)   The UEM server shall generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. (DISA UEM Server SRG: SRG-APP-000266-UEM-000151)

(2)   The UEM server shall reveal error messages only to the ISSO. (DISA UEM Server SRG: SRG-APP-000267-UEM-000152)

(3)   Refer to IRM 10.8.1 for additional guidance on Information Input Validation.

10.8.26.3.19.6
(04-25-2022)
SI-13 Predictable Failure Prevention

(1)   The UEM server shall, when a component failure is detected, activate an organization-defined alarm and/or automatically shut down the application or the component. (DISA UEM Server SRG: SRG-APP-000268-UEM-000153)

(2)   Refer to IRM 10.8.1 for additional guidance on Predictable Failure Prevention.

10.8.26.3.20
(04-25-2022)
SR - Supply Chain Risk Management

(1)   Refer to IRM 10.8.1 for guidance on Supply Chain Risk Management.

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **10.8.26.3.20**
Any line marked with a #
is for **Official Use Only**

This Page Intentionally Left Blank

#
#

#
#
#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#

Exhibit 10.8.26-2   (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
A Advanced Encryption Standard (AES)	A symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers: AES-128, AES-192, and AES-256. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192, and 256 bits, respectively.
Authorizing Official (AO)	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to an agency.
B	
BIOS (Basic Input/Output System)	Software stored on a small memory chip on a computer's motherboard that loads prior to the operating system and instructs the computer on how to perform a number of basic functions such as booting and keyboard controls.
Bluetooth	A proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices, creating wireless personal area networks (WPANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. A Bluetooth piconet is an ad hoc network linking a user group of devices using Bluetooth technology protocols to allow one master device to interconnect with up to seven active slave devices (because a three-bit MAC address is used). Up to 255 further slave devices can be inactive, or parked, which the master device can bring into active status at any time. Piconet range varies according to the class of the Bluetooth device. Data transfer rates vary between about 200 and 2100 kilobits per second (kbit/s) at the application.
Bring Your Own Device (BYOD)	Bring Your Own Device is a concept that allows employees to utilize their personally owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices.

Exhibit 10.8.26-2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Exhibit 10.8.26-2 (Cont. 1) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
Bluetooth Service Level	For Security Mode 4, the Bluetooth specification defines five levels of security for Bluetooth services for use during Secure Simple Pairing. The service security levels are as follows: • Service Level 4 – Requires MITM protection and encryption using 128-bit equivalent strength for link and encryption keys; user interaction is acceptable. • Service Level 3 – Requires MITM protection and encryption; user interaction is acceptable. • Service Level 2 – Requires encryption only; MITM protection is not necessary. • Service Level 1 – MITM protection and encryption not required. Minimal user interaction. • Service Level 0 – No MITM protection, encryption, or user interaction required.
BR	Basic Rate.
C Commercial Mobile Device (CMD)	A subset of Portable Electronic Devices (PEDs) that provides one or more commercial wireless interfaces along with a compact user input interface (Touch Screen, Miniature Keypad, etc.) and excludes PEDs running a multi-user operating system (Windows OS, Mac OS, etc.). This definition includes, but is not limited to smart phones, tablets, and e-readers.
Computer Security Incident Response Center (CSIRC)	Responsible for monitoring the IRS network 24 hours a day year-round for cyber attacks and computer vulnerabilities and for responding to various security incidents such as the theft of a laptop computer.
Controlled Unclassified Information (CUI)	A new category of unclassified categories issued in a directive on May 9, 2008, by President George W. Bush. CUI replaces categories such as For Official Use Only (FOUO), Sensitive But Unclassified (SBU) and Law Enforcement Sensitive (LES) categories. Refers to unclassified information that is to be protected from public disclosure.

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **Exhibit 10.8.26-2**
Any line marked with a #
is for **Official Use Only**

Exhibit 10.8.26-2 (Cont. 2) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
D	
Defense Information Systems Agency (DISA)	An agency composed of military, federal civilian, and contractors. DISA provides IT and communications support to the President, Secretary of Defense, the military services, the combatant commands, and any individual or system contributing to the defense of the United States.
DRBG	Deterministic Random Bit Generators
E	
Encryption	Any procedure used in cryptography to convert plaintext into ciphertext to prevent anyone but the intended recipient from reading that data.
Enterprise Lifecycle (ELC)	The dynamic, iterative process of changing the enterprise over time by incorporating new business processes, new technology, and new capabilities, as well as maintenance, disposition and disposal of existing elements of the enterprise.
ESP	Enterprise Standards Profile.
F Federal Information Processing Standard (FIPS)	Publicly announced standardizations developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract.
G GFE	Government Furished Equipment.
Global Positioning System (GPS)	A space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.
GMT	Greenwich Mean Time
H HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure.
I	
Information Technology (IT)	The application of computers and telecommunications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

Exhibit 10.8.26-2 (Cont. 3) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
iOS (previously iPhone OS)	A mobile operating system developed and distributed by Apple Inc.
IPSec	Internet Protocol Security
Infrared (IR)	Uses pulses of infrared light to transmit data from one device to another. This Infrared light is not visible for the human eye. The Infrared technology has a signal range of about 10 yards and requires line-of-sight.
IRM	Internal Revenue Manual.
IRS	Internal Revenue Service.
ISSO	Information System Security Officer
K KDF	Key Derivation Functions
M MITM	Man-in-the-middle.
Microsoft Intune Company Portal	An application that allows employees to access Outlook, Teams, M365, etc. on their mobile devices.
Mobile Devices/ Portable Electronic Devices (PEDs)	Mobile devices/portable electronic devices have computing and wireless or Local Area Network (LAN) connectivity capabilities. These include, but are not limited to: laptops with wireless capabilities, cellular/personal communication system devices, audio/video/data recording or playback devices, scanning devices, remote sensors, messaging devices, (for example, Blackberries, Palm Pilots, Pocket PCs, iPhones, iPads), and two-way radios.
Mobile Device Management (MDM)	Software that secures, monitors, manages and supports devices deployed across mobile operators, service providers and enterprises.
Multimedia Messaging Service (MMS)	A standard way to send messages that include multimedia content to and from mobile phones.
N National Institute of Standards and Technology (NIST)	The federal technology agency that works with industry to develop and apply technology, measurements, and standards.
O Operating System (OS)	A collection of software that manages computer hardware resources and provides common service for computer programs.

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Internal Revenue Manual

Exhibit 10.8.26-2

Exhibit 10.8.26-2 (Cont. 4) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
P PC	Personal Computer
Peripheral Device	A device that connects directly to a computer or other digital device that does not contribute to the computer's primary function, such as computing. It helps end users access and use the functionalities of a computer. A peripheral device is also called a peripheral, computer peripheral, input-output device, or I/O device.
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.
PIM	Personal Information Management.
PRNG	Pseudo Random Number Generator.
Public Key Infrastructure (PKI)	A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an internet transaction.
R Radio Frequency (RF)	Data transmission technology which is based on electromagnetic radio waves. The advantage of RF is that this technology has a wider signal range, which can be up to 30 yards. RF can go through walls and there is no need to point the remote to the device, as it does not require to be in line-of-sight.
Risk Based Decision (RBD)	RBDs documents various information including the finding or risk, it's impact, mitigating factors and environment to effectively evaluate the impact of accepting that risk.
RNG	Random Number Generator.

Exhibit 10.8.26-2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)

Exhibit 10.8.26-2 (Cont. 5) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
S	
Sanitization	The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Secure Sockets Layer (SSL)	Cryptographic protocols that are designed to provide communication security over the Internet.
Security Assessment Report (SAR)	Reflects assessment activities conducted by assessors to determine security control effectiveness based on modifications to the security plan and deployed controls.
Security Assessment Services (SAS)	Responsible for identifying any security risk and documenting the assessment of risk a SAR.
Security Technical Implementation Guide (STIG)	A methodology for standardized secure installation and maintenance of computer software and hardware.
Sensitive But Unclassified (SBU) Information	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.
Sensitive Information	Information in which the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act), but has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept protected in the interest of national defense or foreign policy. Examples of such sensitive information include personal financial information and information that discloses law enforcement investigative methods. Other particular classes of information may have additional statutory limits on disclosure that require that information to also be treated as sensitive. Examples include tax information, which is protected by Section 6103 of the IRC (26 U.S.C. § 6103) and advanced procurement information, protected by the Procurement Integrity Act (41 U.S.C. § 423).

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **Exhibit 10.8.26-2**
Any line marked with a #
is for **Official Use Only**

Exhibit 10.8.26-2 (Cont. 6) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
Short Messaging Service (SMS)	A text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices.
Smart Card Reader (SCR)	An electronic device that reads smart cards. A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use.
Smartphone	A mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone. Smart-phones combine the functions of a personal digital assistant (PDA), camera, and mobile phone. They also typically include GPS, touchscreens, web-browsing capabilities, and include a mobile operating system (mobile OS) (e.g., Android OS and Apple iOS).
SRG	Security Requirements Guide.
SSH	Secure Shell Protocol
SSID	Service Set Identifier.
Standard Operating Procedures (SOP)	Established or prescribed methods to be followed routinely for the performance of designated opera-tions or in designated situations.
Systems Development Life Cycle (SDLC)	A process of creating or altering information systems, and the models and methodologies that people use to develop these systems.
T Tablet	.A tablet computer (tablet) is a mobile computer, larger than a mobile phone or mobile computing device , integrated into a flat touchscreen and primarily operated by touching the screen rather than using a physical keyboard. It often uses an onscreen virtual keyboard, a passive stylus pen, or a digital pen. Besides having most PC capabilities, popular typical tablet computers include wireless Internet browsing functions, potential cellular functions, GPS navigation, and video camera functions.. In many ways, the functions and purposes of laptops, tablets, and smartphones overlap.
TLS	Transport Layer Security

Exhibit 10.8.26-2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)

Exhibit 10.8.26-2 (Cont. 7) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
Treasury Directive Publication (TD P)	Documents that provide a baseline of IT security standards that apply to the Department of the Treasury bureaus, departmental offices (DO), Office of the Inspector General (OIG), and the Treasury Inspector General for Tax Administration (TIGTA), hereafter referred to collectively as bureaus.
Treasury Inspector General for Tax Administration (TIGTA)	Provides oversight of the Department of Treasury matters involving Internal Revenue Service (IRS) activities, the IRS Oversight Board and the IRS Office of Chief Counsel.
<u>U</u> UEM	Unified Endpoint Managment
UNS	User Network Services
UTC	Coordinated Universal Time
<u>V</u> Virtual Private Network (VPN)	A computer network that links two computers or devices through an underlying local or wide area network, while encapsulating the data and keeping it private. It is comparable to a pipe within a pipe. Even though the outer pipe contains the inner one, the inner pipe has a wall that blocks other traffic in the outer pipe from mixing with the inner traffic. To the rest of the network, the VPN traffic just looks like another traffic stream.
<u>W</u> Wide Area Network (WAN)	A network that covers a broad area (i.e., any tele-communications network that links across metropolitan, regional, or national boundaries) using private or public network transports.
Wi-Fi	Wireless Fidelity.
Wi-Fi Protected Access (WPA)	A security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.
WIPE	A command or series of commands that resets the mobile device to its default factory condition and deletes all user data, including user-installed applications, stored on the device
Wireless	A technology that enables devices to communicate without physical connections (without requiring network or peripheral cabling).
Wireless Client	A system or device that connects to an access point or another client directly via wireless connection.

Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Internal Revenue Manual

Exhibit 10.8.26-2

Exhibit 10.8.26-2 (Cont. 8) (11-06-2023)
Glossary and Acronyms

Term	Definition or Description
Wireless Local Area Network (WLAN)	Links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet.

Exhibit 10.8.26-2   Internal Revenue Manual   Cat. No. 49826K (11-06-2023)
Any line marked with a #
is for **Official Use Only**

Exhibit 10.8.26-3   (04-25-2022)
References

IRS Publications

- IRM 1.4.6 , *Resource Guide for Managers, Managers Security Handbook*.
- IRM 10.2.x , *Physical Security Program* series.
- IRM 10.2.1 , *Physical Security Program, Physical Security*.
- IRM 10.2.8 , *Physical Security Program, Incident Reporting*.
- 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 10.8.27 , *Information Technology (IT) Security, Personal Use of Government Furnished Information Technology Equipment and Resources*.
- IRM 10.8.50 , *Information Technology (IT) Security, Service-wide Security Patch Management*.
- IRM 10.8.52 , *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*.
- IRM 10.8.54 , *Information Technology (IT) Security, Minimum Firewall Administration Requirements*
- IRM 10.9.1 , *National Security Information*.

Department of the Treasury Publications

- TD P 85-01, Version 3.1.2 *Treasury Information Technology (IT) Security Program*, November 03, 2020

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020.
- NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014 (includes updates as of December 18, 2014)
- NIST SP 800-121 Rev 2, Guide to Bluetooth Security, May 2017

Defense Information Systems Agency (DISA) Publications

- DISA UEM Agent SRG V1R1, January 3, 2021
- DISA UEM Server SRG V1R1, January 3, 2021
- STIGs are used as a basis for producing IRS Exhibit Checklists. The security checklists are updated as DISA releases updated guidance and are posted on the IRS Security Control Exhibit SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to the Security Requirements Checklists exhibit for additional information.
- DISA security guides are available at: *https://public.cyber.mil/stigs/*

Cat. No. 49826K (11-06-2023)   Internal Revenue Manual   **Exhibit 10.8.26-3**
Any line marked with a #
is for **Official Use Only**