MANUAL TRANSMITTAL

10.8.11

Department of the Treasury
Internal Revenue Service

NOVEMBER 3, 2023

EFFECTIVE DATE

(11-03-2023)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.11, *Information Technology (IT) Security, Application Security Policy.* The purpose of this IRM is to provide guidance and establish requirements necessary to implement and manage IT security for applications within the IRS.

MATERIAL CHANGES

(1) IRM 10.8.11.3, Roles and Responsibilities - Moved to align with IRM 1.11.2 requirements.

(2) IRM 10.8.11.4, Program Management and Review - Moved to align with IRM 1.11.2 requirements.

(3) IRM 10.8.11.5, Program Control - Updated to align with IRM 1.11.2.

(4) IRM 10.8.11.6, Terms and Acronyms - Changed Glossary to Terms and merged it with Acronyms.

(5) IRM 10.8.11.7 Related Resources - Was added to align with IRM 1.11.2 requirements.

(6) Editorial changes made throughout the IRM for clarity. Reviewed and updated plain language, grammar, titles, website addresses, legal references and IRM references.

EFFECT ON OTHER DOCUMENTS

This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance*; IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.
IRM 10.8.11, dated July 26, 2022 is superseded.

AUDIENCE

IRM 10.8.11 shall be distributed to all personnel responsible for overseeing, managing, and implementing application security for IRS information and information systems. The Application Security Policy will consist of, but will not be limited to, agency defined requirements, authoritative guidance, legislative mandates, and national standards. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.11
Application Security Policy

Table of Contents

10.8.11.1 Program Scope and Objectives
10.8.11.1.1 Background
10.8.11.1.1.1 Scope
10.8.11.1.1.2 Objectives
10.8.11.1.2 Authority
10.8.11.1.3 Roles and Responsibilities
10.8.11.1.4 Program Management and Review
10.8.11.1.5 Program Control
10.8.11.1.6 Terms and Acronyms
10.8.11.1.7 Related Resources
10.8.11.2 IT Security Controls

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

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

Exhibits

#

#

#

10.8.11.1
(11-03-2023)
Program Scope and Objectives

(1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage security controls and guidance for the use of applications within the Internal Revenue Service (IRS).

a. This manual is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS applications.

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

(3) **Audience:** The provisions within this manual apply to:

a. All offices and business, operating, and functional units within the IRS.
b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, that use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system:

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

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

(6) **Program Goals:** Security Policy is responsible for the development and maintenance of IRS's enterprise information technology security policies. The IRM 10.8. 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), the Department of the Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, and the National Archives and Records Administration (NARA).

10.8.11.1.1
(07-26-2022)
Background

(1) IRM 10.8.11 defines security controls for application programs. An application is a software program that is hosted by an information system and is designed to perform a specific function directly for the user or, in some cases, for another application. Application programs can be executed without access to system control, monitoring, or administrative privileges.

(2) IRM 10.8.11 is part of the Security, Privacy, and Assurance policy family, IRM Part 10 Series for IRS Information Technology Cybersecurity.

10.8.11.1.1.1
(07-26-2022)
Scope

(1) This IRM applies to all IRS information and systems, which include IRS production, development, test, and contractor systems. For information systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, Classified National Security Information (NSI), for additional procedures for protecting classified information.

(2) Unless approved by the CIO, given the associated security challenges, lack of security solutions and high implementation cost, the use of emerging technologies that have not been evaluated by the federal government for their national security impacts is prohibited. (E.O. 13960 Sec 2 (c), Sec 3 (b); 44 USC 3551 Purposes(6))

(3) For a list of Organizational Common Controls (OCC), contact Security Risk Management (SRM).

(4) Security Requirements Checklists:

a. Security Requirements Checklists, if accompanying this IRM, serve as the secure configuration benchmark and are developed in accordance with NIST Special Publication (SP) 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers.*
b. IRMs with accompanying checklists contain a checklist with general security requirements (e.g., Defense Information Systems Agency (DISA) Security Requirements Guide (SRG)), as well as checklists with platform or technology specific requirements (e.g., Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks). In the event a platform or technology specific checklist is not available, the general security requirements checklist shall be used (e.g., Database (General), Operating System (General), Router (General)).
c. Security Requirements Checklists shall be used in addition to the requirements within this IRM.
d. In the event of a conflict between a checklist and this IRM, excluding Treasury's defined requirements, the requirement(s) from the checklist shall take precedence.
e. Implementation of Security Requirements Checklists is required (CM - 6).
f. Refer to the Security Requirements Checklist exhibit for additional guidance.

(5) In the event there is a discrepancy between this IRM, the Checklists and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this IRM are more restrictive or otherwise noted.

10.8.11.1.1.2
(08-10-2021)
Objectives

(1) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
b. Prevent unauthorized access to IRS assets.
c. Enable IRS IT computing environments to meet the security requirements of this IRM and support the business needs of the organization.

(2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.

(3) To configure less restrictive requirements requires a risk-based decision. Refer to the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

10.8.11.1.2
(08-10-2021)
Authority

(1) All IRS information systems and applications shall be compliant with executive orders (E.O.s), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of the Treasury, and IRS guidelines as they apply.

10.8.11.1.3
(11-03-2023)
Roles and Responsibilities

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

10.8.11.1.4
(11-03-2023)
Program Management and Review

(1) Security Policy program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.

10.8.11.1.5
(11-03-2023)
Program Control

(1) Each IRM in the 10.8 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 weekly report identifying security policies and security requirement checklists that have recently been revised or are in the process of being revised.

10.8.11.1.6
(11-03-2023)
Terms and Acronyms

(1) Refer to Exhibit # 10.8.11-2 # for a list of terms, acronyms, and definitions.

10.8.11.1.7
(11-03-2023)
Related Resources

(1) Refer to Exhibit # 10.8.11-3 # for a list of related resources and references.

10.8.11.1.8
(08-10-2021)

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

10.8.11.2
(08-10-2021)
IT Security Controls

#
#
#
#

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

#
#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#

#
#

#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#

#
#
#

#
#
#

#
#

#
#

#
#

#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#

#
#
#
#

#
#
#

#
#

#
#
#

#
#
#

#
#

#

#
#
#
#
#

#
#
#

#
#

#
#
#
#

#

#

#
#
#
#

#
#
#
#
#
#
#
#
#

Any line marked with a #
is for **Official Use Only**

#
#

#
#
#

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#

#

#
#
#
#
#

#
#

#
#

#
#
#

#
#

#

#
#
#
#
#

#
#

#

#
#
#
#
#

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

#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

#
#
#

#
#

#

#
#
#

#
#
#
#
#
#

#
#
#

#

#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#

#
#

#
#
#
#
#
#

#
#

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

#
#
#
#
#

#
#
#

#
#

#
#
#

#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#

#
#
#

#
#
#
#

This Page Intentionally Left Blank

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#
#

#
#
#
#

#

#
#
#

#

#
#
#
#
#
#
#
#
#
#

#

#
#

#

#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#

#

#
#
#
#
#