



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.21

NOVEMBER 9, 2023

EFFECTIVE DATE

(11-09-2023)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.21, *Information Technology (IT) Security, Database Security Policy*.

MATERIAL CHANGES

- (1) IRM 10.8.21.1(1)a, Program Scope and Objectives - Updated text to align with Security Policy boilerplate.
- (2) IRM 10.8.21.1(2), Program Scope and Objectives - Updated text to align with Security Policy boilerplate.
- (3) IRM 10.8.21.1(3), Program Scope and Objectives - Updated text to align with Security Policy boilerplate.
- (4) IRM 10.8.21.1(5), Program Scope and Objectives - Updated Program Owner from “Architecture and Implementation” to “Cybersecurity, Threat Response and Remediation.”
- (5) IRM 10.8.21.1(6), Program Scope and Objectives - Updated text to align with Security Policy boilerplate.
- (6) IRM 10.8.21.1.1.1, Scope - Subsection removed; content relocated elsewhere in the document or removed to align with Security Policy boilerplate.
- (7) IRM 10.8.21.1.1.2, Objectives - Subsection removed; content relocated elsewhere in the document or removed to align with Security Policy boilerplate.
- (8) IRM 10.8.21.1.2(1), Authority - Text updated to align with Security Policy boilerplate.
- (9) IRM 10.8.21.1.3, Roles and Responsibilities - Subsection renumbered from 10.8.21.2 to align with Security Policy boilerplate and SPDER internal controls structure.
- (10) IRM 10.8.21.1.3.1, Application Developer - Subsection renumbered due to parent section (Roles and Responsibilities) being renumbered.
- (11) IRM 10.8.21.1.4, Program Management and Review - New subsection added to align with SPDER internal controls.
- (12) IRM 10.8.21.1.5, Program Controls - New subsection added to align with SPDER internal controls.
- (13) IRM 10.8.21.1.5(3)&(5), Program Controls - Text added from now deleted “Scope” subsection.
- (14) IRM 10.8.21.1.5(4), Program Controls - Text added from now deleted “Objectives” subsection.
- (15) IRM 10.8.21.1.6, Terms and Acronyms - New subsection added to align with SPDER internal controls.
- (16) IRM 10.8.21.1.7, Related Resources, New subsection added to align with SPDER internal controls.
- (17) IRM 10.8.21.2, Risk Acceptance and Risk-Based Decisions - Subsection number updated to align with Security Policy boilerplate.

- (18) IRM 10.8.21.2(2), Risk Acceptance and Risk-Based Decisions - Text updated to align with Security Policy boilerplate; URL to Risk Based Decisions SOP updated.
- (19) IRM 10.8.21.3, IT Security Controls - Text updated to align with Security Policy boilerplate; text (2) and (3) moved from the now deleted “Objectives” subsection.
- (20) IRM 10.8.21.3.7.2(1), (2) & (7), IA-5 Authenticator Management - Note added regarding the applicability of the requirement for systems not able to implement Multi-factor authentication.
- (21) IRM 10.8.21.3.7.2(6), IA-5 Authenticator Management - Note updated to indicate that system owners define the time period for cached authenticators.
- (22) IRM 10.8.21.3.7.6(1), IA-11 Re-authentication - Updated requirement to end with “in accordance with IRM 10.81.” and removed subsection ‘a’ as it repeats information from IRM 10.8.1.
- (23) IRM 10.8.21.3.19.2(3), SI-10 Information Input Validation - Removed subsection ‘a’ and added a note to view the requirement in the Security Requirements Checklist for the additional information.
- (24) IRM Exhibit 10.8.21-1(1), Security Requirements Checklists - Text added from the now deleted “Scope” subsection, other text renumbered as needed.
- (25) IRM Exhibit 10.8.21-1(2), Security Requirements Checklists - Updated the URL to the Security Policy SharePoint website.
- (26) IRM Exhibit 10.8.21-1(2)b, Security Requirements Checklists - Added ‘Maria’ under the products that security checklists are available for.
- (27) IRM Exhibit 10.8.21-1(4), Security Requirements Checklists - Text updated to align with Security Policy boilerplate, clarifies the circumstances when checklists for technologies are no longer updated.
- (28) IRM Exhibit 10.8.21-2, Terms and Acronyms - Subsection renamed to align with SPDER internal controls name and items added as required in the table.
- (29) IRM Exhibit 10.8.21-3, Related Resources - Updated name of subsection to align with SPDER internal controls.
- (30) IRM Exhibit 10.8.21-3(4), Related Resources - Updated dates for NIST SP 800-53 Rev 5 and NIST SP 800-53A Rev 5 and the revision number for NIST SP 800-53A to Rev 5.
- (31) IRM Exhibit 10.8.21-3(5), Related Resources - Database Security Requirements Guide Release number updated, text updated to align with Security Policy boilerplate.
- (32) IRM Exhibit 10.8.21-3(6), Related Resources - Updated text to align with Security Policy, added additional URL to IBM DB2 for zOS 12.
- (33) IRM Exhibit 10.8.21-3(8), Related Resources - Updated text to align with Security Policy boilerplate.
- (34) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 10.8.21, dated September 23, 2021, and all prior versions of IRM 10.8.21. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*; and IRM 10.8.2 *Information Technology (IT) Security, Security Roles and Responsibilities*.

AUDIENCE

IRM 10.8.21 shall be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. This policy applies to all employees, contractors and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.21.1
(11-09-2023)
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 databases within the Internal Revenue Service (IRS).
 - a. This policy 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 database systems.
- (2) **Purpose of the Program:** Develop and publish security policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this policy apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process or transmit IRS information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer
- (5) **Program Owner:** Cybersecurity, Threat Response and Remediation (an organization within Cybersecurity)
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of information and information systems.

10.8.21.1.1
(11-30-2020)
Background

- (1) This IRM establishes a comprehensive policy to implement the minimum security controls to safeguard databases within the IRS organization.
- (2) IRM 10.8.21 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.21.1.2
(11-09-2023)
Authority

- (1) All IRS systems and applications must 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.

10.8.21.1.3
(11-09-2023)
Roles and Responsibilities

- (1) IRM 10.8.2, *Information Technology (IT), 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.
- (2) The supplemental roles and responsibilities provided below are specific to the implementation of a Database Management System (DBMS).

10.8.21.1.3.1
(11-09-2023)
Application Developer

- (1) The application developer role is used to assign required privileges to developer accounts on a development database. Application developers must not be permitted access to production databases, except as specified within the Security Requirements Checklists for this IRM and IRM 10.8.1.

10.8.21.1.4
(11-09-2023)

**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.
 - 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), Software Development Life Cycle (SDLC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.21.1.5
(11-09-2023)

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, Defense Information Systems Agency (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 databases 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.

#

#

#

#

#

#

Exhibit 10.8.21-2 (11-09-2023)**Terms and Acronyms**

Term	Definition or description
AO	Authorizing Official
Application Developers	Refer to Developers
Authorized or Unauthorized Personnel	Applies to all IRS personnel being authorized or not authorized to perform a particular action.
CA	Certification Authority
CIS	Center for Internet Security
CRL	Certificate Revocation List
CSIRC	Computer Security Incident Response Center
DASD	Direct Access Storage Device
DBA	Database Administrator
DBMS	Database Management System
Developers or Application Developers	Refers to “Program Developers/Programmers” and “Web Developers” as defined in IRM 10.8.2. Note: This does not refer to database administrators (DBAs), who may assist Developers.
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
Discretionary Access Control (DAC)	A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
DML	Data Manipulation Language
EA	Enterprise Architecture
ESAT	Enterprise Security Audit Trails
ESP	Enterprise Standards Profile
FIFO	First-In-First-Out
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GMT	Greenwich Mean Time
HTML	Hypertext Markup Language

Exhibit 10.8.21-2 (Cont. 1) (11-09-2023)
Terms and Acronyms

IBM	International Business Machines
IP	Internet Protocol
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
OCSP	Online Certificate Status Protocol
OS	Operating System
OMB	Office of Management and Budget
OUO	Official Use Only
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RBD	Risk Based Decision
RIM	Records and Information Management
Risk Based Decisions	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive).
SA	System Administrator
SBU	Sensitive But Unclassified
SOP	Standard Operating Procedure
SP	Special Publication
SRG	Security Requirements Guide

Exhibit 10.8.21-2 (Cont. 2) (11-09-2023)
Terms and Acronyms

SRM	Security Risk Management
SSP	System Security Policy
STIG	Security Technical Implementation Guide
TD	Treasury Directive
Unauthorized Personnel	Refer to Authorized Personnel
UTC	Coordinated Universal Time
XML	Extensible Markup Language

