



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

1.15.6

FEBRUARY 26, 2025

EFFECTIVE DATE

(02-26-2025)

PURPOSE

- (1) This transmits revised IRM 1.15.6, Records and Information Management, Managing Electronic Records.

MATERIAL CHANGES

- (1) The content in this IRM section is revised, reorganized, and renumbered for clarity.
- (2) IRM 1.15.6.1 - Program Scope and Objectives - Included missing internal controls and rearranged content to conform to a standardized format, resulting in some IRM subsections being renumbered accordingly.
- (3) IRM 1.15.6.1.1 - Background - Added content on OMB/NARA M-23-07, Update to Transition to Electronic Records.
- (4) IRM 1.15.6.1.2 - Authority - Added reference to OMB/NARA M-23-07, Update to Transition to Electronic Records and reference to the NARA Universal Electronic Records Management Requirements for all agencies. Also added 36 Code of Federal Regulations (CFR) 1236, Subpart D - Digitizing Temporary Federal Records, Subpart E - Digitizing Permanent Federal Records, and Subpart F - Transfer Metadata.
- (5) IRM 1.15.6.1.4 - Program Management and Review - Added a new subsection on how the records management program is managed, and how the effectiveness and objectives are measured. Added the following new forms and their usage:
 - Form 14377, Records and Information Management Virtual Program Review Self Assessment Checklist
 - Form 14377-A, IRS Records and Information Management (RIM) Evaluation Checklist
 - Form 15407, Electronic Recordkeeping System Assessment (eRSA)
 - Form 15407-A, One Solution Delivery Lifecycle (OneSDLC) Records and Information Management (RIM) Checklist
 - Form 15408, Digitization Validation Assessment
 - Form 15408-A, Itemized Audit Digitization Quality Review Sheet
- (6) IRM 1.15.6.1.5 - Program Controls - Added a new subsection describing the records management controls that oversee the program.
- (7) IRM 1.15.6.1.6 - Acronyms/Terms/Definitions - Combined content from the Acronyms and Terms subsection with the Definition of Records subsection to conform to internal controls. Incorporated content from the Interim Guidance Memorandum PGLD-01-1223-0009, Disposal of Original Source Material After Digitization of Temporary Records, dated December 21, 2023. Renumbered the subsequent subsections accordingly.
- (8) IRM 1.15.6.1.7 - Related Resources - Added content on OMB/NARA M-23-07, Update to Transition to Electronic Records and updated the other resources.
- (9) IRM 1.15.6.2 - Basic Electronic Records Management Definitions - Expanded the list of definitions for electronic records management and alphabetically rearranged the list accordingly.

- (10) IRM 1.15.6.4 - Electronic Records - Added new subsection explaining electronic records.
- (11) IRM 1.15.6.5 - Metadata - Added new subsection explaining metadata capturing, maintenance, and electronic recordkeeping systems.
- (12) IRM 1.15.6.6 - Scheduling Electronic Records - Adjusted subsection title and updated content.
- (13) IRM 1.15.6.7 - Creation, Use, and Maintenance of Structured Electronic Data - Updated content incorporating implementation of electronic records management in systems design, development, production, use or storage of official records, and data files. Added new content and use of Form 15407 , Electronic Recordkeeping System Assessment (eRSA) and Form 15407-A , One Solution Delivery Lifecycle (OneSDLC) Records and Information Management (RIM) Checklist.
- (14) IRM 1.15.6.8 - Creation, Use, and Maintenance of Unstructured Electronic Data - Updated content on managing unstructured data and developing, maintaining, and publishing automated disposition policies.
- (15) IRM 1.15.6.9 - Managing Electronic Mail Records - Updated content on the IRS role-based approach for managing electronic mail records.
- (16) IRM 1.15.6.9.3 - Email Sent or Received Using Government-issued Communications Tools - Removed some content that is relocated to IRM 1.15.6.9.4.
- (17) IRM 1.15.6.9.4 - Email Created Using Personal or Non-IRS Communications Tools (Bring Your Own Device (BYOD) Program) - Updated section title for IRM 10.8.26, as Wireless and Mobile Device Security Policy and included some content previously located in IRM 1.15.6.9.3.
- (18) IRM 1.15.6.10 - Judicial Use of Electronic Records - Updated content on electronic records used as evidence.
- (19) IRM 1.15.6.11 - Security of Electronic Records - Updated content on classified electronic records stored on approved systems.
- (20) IRM 1.15.6.12 - Disposition of Electronic Records - Expanded content on electronic records disposition.
- (21) IRM 1.15.6.13 - Transfer of Permanent Records to NARA - Removed content no longer applicable.
- (22) IRM 1.15.6.13.1 - Transfer Forms for Permanent Records - Updated content on transfer of permanent records to the National Archives and Records Administration (NARA).
- (23) IRM 1.15.6.13.4.3 - File Transfer Protocol (FTP) - Removed content no longer applicable and updated content accordingly.
- (24) IRM 1.15.6.13.4.4 - Electronic Storage Media Maintenance Requirements for Permanent Records - Expanded content on maintaining areas with electronic storage media for permanent records.
- (25) IRM 1.15.6.14 - Disposal of Temporary Electronic Records - Updated subsection to explain the handling of born-digital and digitized source records.
- (26) IRM 1.15.6.16 - Use of Collaboration Tools - Updated content on managing records using collaboration tools.
- (27) IRM 1.15.6.16.1 - Agency-approved Electronic Messaging - Updated the subsection title, adjusted content to include Microsoft 365 for instant messaging, and removed some content that is no longer applicable. Incorporated Interim Guidance Memorandum PGLD-01-0324-0010, Text Messaging, dated March 11, 2024, that allows limited automation, system-generated one-way text messaging with

generic, non-sensitive information as a provision of the IRS Inflation Reduction Act Strategic Operating Plan and clarified privacy requirements for phone conversations about sensitive information.

- (28) IRM 1.15.6.16.2 - Preserving Electronic Messages - Deleted subsection as the content is no longer applicable.
- (29) IRM 1.15.6.17 - Digitization Requirements - Expanded content on digitization requirements and use of new forms, as follows:
 - Form 15407, Electronic Recordkeeping System Assessment (eRSA)
 - Form 15407-A, One Solution Delivery Lifecycle (OneSDLC) Records and Information Management (RIM) Checklist
 - Form 15408, Digitization Validation Assessment
 - Form 15408-A, Itemized Audit Digitization Quality Review Sheet
- (30) IRM 1.15.6.17.1 - Digitizing Temporary Records - Expanded content on digitizing temporary records and use of the new Form 15408, Digitization Validation Assessment.
- (31) IRM 1.15.6.17.2 - Digitizing Permanent Records - Added new content on digitizing permanent records.
- (32) Exhibit 1.15.6-1 - Common Questions about Email - Expanded content.
- (33) Exhibit 1.15.6-2 - Common Questions about Electronic Messaging - Removed content no longer applicable.
- (34) IRM references, website links, and editorial updates were made throughout this IRM section.

EFFECT ON OTHER DOCUMENTS

IRM 1.15.6, dated March 18, 2021, is superseded. This IRM incorporates Interim Guidance Memorandum on Disposal of Original Source Material After Digitization of Temporary Records, PGLD-01-1223-0009, dated 12-23-2023 and Interim Guidance Memorandum on Text Messaging, PGLD-01-0324-0010, dated 03-11-2024.

AUDIENCE

All IRS divisions and functions

Michael J. Oser
Acting Director, Identity and Records Protection (IRP)
Privacy, Governmental Liaison and Disclosure (PGLD)

1.15.6
Managing Electronic Records

Table of Contents

- 1.15.6.1 Program Scope and Objectives
 - 1.15.6.1.1 Background
 - 1.15.6.1.2 Authority
 - 1.15.6.1.3 Responsibilities
 - 1.15.6.1.4 Program Management and Review
 - 1.15.6.1.5 Program Controls
 - 1.15.6.1.6 Acronyms/Terms/Definitions
 - 1.15.6.1.7 Related Resources
- 1.15.6.2 Basic Electronic Records Management Definitions
- 1.15.6.3 Responsibility for Issuance of Guidance
- 1.15.6.4 Electronic Records
- 1.15.6.5 Metadata
- 1.15.6.6 Scheduling Electronic Records
- 1.15.6.7 Creation, Use, and Maintenance of Structured Electronic Data
- 1.15.6.8 Creation, Use, and Maintenance of Unstructured Electronic Data
- 1.15.6.9 Managing Electronic Mail Records
 - 1.15.6.9.1 Email Sent or Received Using Organizational Mailboxes
 - 1.15.6.9.2 Federal Advisory Committee Act (FACA) Email Records
 - 1.15.6.9.3 Email Sent or Received Using Government-issued Communications Tools
 - 1.15.6.9.4 Email Created Using Personal or Non-IRS Communications Tools (Bring Your Own Device (BYOD) Program)
 - 1.15.6.9.5 Email Created Using Personal or Non-IRS Communications Tools (not part of the BYOD Program)
 - 1.15.6.9.6 Encrypted Email
 - 1.15.6.9.7 Litigation Holds
 - 1.15.6.9.8 System Backups
- 1.15.6.10 Judicial Use of Electronic Records
- 1.15.6.11 Security of Electronic Records
- 1.15.6.12 Disposition of Electronic Records
- 1.15.6.13 Transfer of Permanent Records to NARA
 - 1.15.6.13.1 Transfer Forms for Permanent Records
 - 1.15.6.13.2 Transfer Documentation for Permanent Records
 - 1.15.6.13.2.1 Sources of the Documentation
 - 1.15.6.13.2.2 Format of the Documentation
 - 1.15.6.13.2.3 Scope of the Documentation

-
- 1.15.6.13.3 Transfer Formats for Permanent Records
 - 1.15.6.13.4 Transfer Media for Permanent Records
 - 1.15.6.13.4.1 Magnetic Tape
 - 1.15.6.13.4.2 Compact Disk, Read Only Memory (CD-ROM) and Digital Video Disk (DVD)
 - 1.15.6.13.4.3 File Transfer Protocol (FTP)
 - 1.15.6.13.4.4 Electronic Storage Media Maintenance Requirements for Permanent Records
 - 1.15.6.14 Disposal of Temporary Electronic Records
 - 1.15.6.15 Use of Social Media
 - 1.15.6.16 Use of Collaboration Tools
 - 1.15.6.16.1 Agency-approved Electronic Messaging
 - 1.15.6.17 Digitization Requirements
 - 1.15.6.17.1 Digitizing Temporary Records
 - 1.15.6.17.2 Digitizing Permanent Records

Exhibits

- 1.15.6-1 Common Questions about Email
- 1.15.6-2 Common Questions about Electronic Messaging

1.15.6.1
(02-26-2025)
Program Scope and Objectives

- (1) **Overview:** Managing electronic records in systems and repositories that meet the requirements listed in this paragraph, ensures the IRS is compliant with the critical records and information management policies and regulations established by the National Archives and Records Administration (NARA) and listed in the Code of Federal Regulations (CFR). IRS adherence to these policies also increases business efficiency and the value of information created. These requirements apply to all IRS electronic recordkeeping systems and unstructured data repositories. At the IRS, repositories must:
 - a. **Store and preserve federal records and associated metadata** - repositories must allow access for users to retrieve and use all records in the repository, until the NARA-approved retention period ends.
 - b. **Manage access and retrieval** - repository administrators must establish appropriate user rights to access, search, and retrieve records, and prevent unauthorized access, modification, or destruction of records.
 - c. **Execute dispositions** - Privacy, Governmental Liaison and Disclosure (PGLD), in coordination with repository owners, administrators, and users, must assign unique identifiers to records, associate electronic records to their respective records schedules, destroy temporary records that are eligible for destruction, identify permanent records and carry out their transfer to NARA, and apply records holds or freezes on dispositions when required.
 - d. **Backup systems** - system administrators must design systems and processes to back up the electronic records using processes and media (system or file) that incorporate the appropriate functions in this section.

Note: System and file backup processes and media do not provide the appropriate recordkeeping functionalities and must not be used as the IRS electronic recordkeeping system.
- (2) **Purpose:** This IRM sets forth policy, assigns responsibilities, and explains requirements for the management of electronic records in accordance with the *Code of Federal Regulations (CFR) Title 36, chapter XII subchapter B*, the *NARA Universal Electronic Records Management (ERM) Requirements*, and the United States Code (USC) Title 44, chapters 29, 31, 33, and 35. This IRM section covers the following:
 - a. Basic requirements for electronic records.
 - b. Creation, maintenance, retention, and disposition of records (including the transfer of permanent electronic records to NARA).
 - c. Usage and preservation of all electronic messages (including email, instant and text messaging platforms) that allow users to send messages in real time or for later viewing and are used to send messages from one account to another account or from one account to many accounts.
 - d. A roles-based management approach to email records management. See IRM 1.15.6.9, Managing Electronic Mail Records.
 - e. Recordkeeping requirements when using personal or non-IRS communication tools to conduct IRS business.
 - f. Basic requirements for digitizing (scanning) temporary and permanent records.
 - g. IRS compliance requirements with the NARA records management policies and regulations, improvement in business efficiency and faster responses to litigation and Freedom of Information Act (FOIA) requests.
- (3) **Audience:** These procedures apply to **all** IRS employees and contractors.

- (4) **Policy Owner:** Director, Identity and Records Protection - Records and Information Management (RIM).
- (5) **Program Owner:** The Records and Information Management (RIM) Program office, under Privacy, Governmental Liaison and Disclosure (PGLD) is the program office responsible for oversight of the Servicewide records management policy.
- (6) **Primary Stakeholders:** The RIM Program office, under PGLD, promotes responsible recordkeeping practices for IRS employees and contractors to follow in accordance with federal laws, regulations, procedures, and NARA guidance.

1.15.6.1.1
(02-26-2025)
Background

- (1) This IRM covers the creation, maintenance, use, and disposition of federal records created using IRS electronic information systems and individual computers/laptops, including electronic mail and other electronic applications.
- (2) Managing records and information in appropriate recordkeeping systems will ensure that the IRS is compliant with all records and information management policies and regulations as established by NARA. Additionally, management of all IRS information, hard copy (also known as analog) and electronic, will improve the IRS's ability to identify the most current information in a timely manner, increase business efficiency, and provide the correct information for litigation and FOIA requests.
- (3) Electronic records must be protected against unauthorized access, use, alteration, alienation, or deletion until the authorized disposition date. Without active management throughout their lifecycle, electronic records are not likely to remain accessible or to be complete and reliable, even over short periods. For these reasons, IRS offices must manage electronic records through the development and implementation of electronic recordkeeping systems that capture, maintain, and provide access to these records over time.
- (4) The information users create and receive day-to-day may or may not be records and users need to delete non-record emails when no longer needed for reference; apply the appropriate retention periods to all information regardless of record status (36 CFR 1222.16, How are non-records managed?). See IRM 1.15.6.1.6, Acronyms/Terms/Definitions, for the definition of records, non-records, and personal materials.
- (5) The Office of Management and Budget (OMB) and NARA jointly issued *OMB/NARA M-23-07*, Update to Transition to Electronic Records. This memo reinforces M-19-21, Transition to Electronic Records and supersedes M-12-18, Managing Government Records Directive. This memo provides key targets for federal agencies to manage permanent and electronic records in electronic format. M-23-07 established a June 30, 2024 cutoff date for sending paper (analog) records to the Federal Records Centers (FRCs) and for sending permanent paper (analog) records to NARA. Limited IRS exceptions to M-23-07 are currently in effect until December 31, 2030.
- (6) The PGLD, RIM Program office will provide assistance and training, where necessary, on implementing the requirements provided in this IRM and for answering any questions relative to IRS's limited exceptions to M-23-07.

1.15.6.1.2
(02-26-2025)
Authority

- (1) 44 USC Chapters 21, 29, 31, and 33
- (2) 36 CFR Chapter XII Subchapter B, Records Management codes
- (3) 36 CFR Chapter XII, Subpart B - Part 1222 - Agency Recordkeeping Requirements
- (4) 36 CFR Chapter XII, Subpart B - Part 1223 - Managing Vital Records
- (5) 36 CFR Chapter XII, Subpart B - Part 1235 - Transfer of Records to the National Archives of the United States
- (6) 36 CFR Chapter XII, Subpart B - Part 1236 - Electronic Records Management
- (7) 36 CFR Chapter XII, Subpart D - Part 1236 - Digitizing Temporary Federal Records
- (8) 36 CFR Chapter XII, Subpart E - Part 1236 - Digitizing Permanent Federal Records
- (9) 36 CFR Chapter XII, Subpart F - Part 1236 - Transfer Metadata
- (10) OMB/NARA M-23-07, Update to Transition to Electronic Records
- (11) OMB/NARA M-19-21, Transition to Electronic Records
- (12) NARA Bulletin 2023-04, Managing Records Created on Collaboration Platforms
- (13) NARA Bulletin 2018-01, Updating NARA Bulletin 2014-04, Format Guidance for the Transfer of Permanent Electronic Records
- (14) NARA Bulletin 2015-04, Metadata Guidance for the Transfer of Permanent Electronic Records
- (15) NARA Bulletin 2015-02, Guidance on Managing Electronic Messages
- (16) NARA Bulletin 2014-06, Guidance on Managing Email
- (17) NARA Bulletin 2014-04, Revised Format Guidance for the Transfer of Permanent Electronic Records
- (18) NARA Bulletin 2014-02, Guidance on Managing Social Media Records
- (19) NARA Bulletin 2013-02, Guidance on a New Approach to Managing Email Records
- (20) NARA Bulletin 2012-02, Guidance on Managing Content on Shared Drives
- (21) Protecting Americans from Tax Hikes (PATH) Act of 2015, Division Q, Title IV, Section 402, *IRS Employees Prohibited from Using Personal Email Accounts for Official Business*
- (22) 5 USC Appendix 2 - Federal Advisory Committee Act (FACA)
- (23) NARA Universal Electronic Records Management Requirements
- (24) OMB Circular No. A-130, Managing Federal Information as a Strategic Resource

1.15.6.1.3
(07-16-2018)
Responsibilities

- (1) This IRM is used by **all** IRS employees and contractors to ensure compliance with electronic records management requirements.

1.15.6.1.4
(02-26-2025)
Program Management and Review

- (1) The RIM Program is evaluated using the following reviews and reports:
- **Records Management Self-Assessment (RMSA):** The annual RMSA asks questions that assess compliance with records management statutes and regulations, as well as the NARA policies and guidance.
 - **Federal Electronic Records and Email Management Reporting:** This report not only evaluates federal agency email management, but it also seeks to assess the current state of all electronic records management at federal agencies (including email and permanent electronic records).
 - **Senior Agency Official for Records Management (SAORM) Annual Report:** This report gathers data on agency progress towards the goals of the OMB/NARA M-23-07, Update to Transition to Electronic Records, and other important records management initiatives as identified by NARA.
 - **Form 14377, Records and Information Management Virtual Program Review Self Assessment Checklist:** This checklist is utilized as a self-assessment tool to assist the field site offices with records management policies and procedures. In addition, it measures RIM goals to stimulate better fiscal management.
 - **Form 14377-A, IRS Records and Information Management (RIM) Evaluation Checklist:** PGLD requires all business unit information resource coordinator (BU/IRC) contacts to complete this form on a quarterly basis. The purpose of the form is to ensure and document IRS recordkeeping compliance as defined by NARA. Completing the Form 14377-A identifies to PGLD:IRP:RIM potential gaps for training opportunities to assist the business unit with their recordkeeping responsibilities.
 - **Form 15407, Electronic Recordkeeping System Assessment (eRSA):** This form is the evaluation method used by the RIM Program office within PGLD to assess if an electronic information system, that produces, uses, or stores official IRS records, is compliant with NARA's scheduling and electronic records management requirements.
 - **Form 15407-A, One Solution Delivery Lifecycle (OneSDLC) Records and Information Management (RIM) Checklist:** This form is used to assist IRS project/system owners with integrating scheduling and system electronic records management (ERM) requirements into the One Solution Delivery Lifecycle (OneSDLC) pathway. The checklist identifies certain points in the SDLC process (allocation, readiness, and execution) to ensure that sound RIM practices are incorporated into the development of its proposed Information Technology (IT) solutions managing official IRS records.
 - **Form 15408, Digitization Validation Assessment:** This form is used to validate that the scheduling, technical specifications, metadata, quality control, repository, and legal constraints digitization requirements have been met before approval can be given to destroy the original source records.
 - **Form 15408-A, Itemized Audit Digitization Quality Review Sheet:** This form is used by quality control reviewers to verify and document that digitized records and associated metadata from digitization projects or ongoing operations comply with quality, accuracy, metadata, and

usability digitization standards listed in Form 15408, the standard operating procedure, or the digitization project plan.

1.15.6.1.5
(02-26-2025)
Program Controls

- (1) **Records Management Mandatory Briefing:** Every IRS employee and contractor must protect the information they handle daily to carry out their job responsibilities. They must annually take the Records Management Mandatory Briefing Integrated Talent Management (ITM) course #62965, Records Management Awareness, to ensure IRS records management is efficient, effective, and compliant with all applicable records management laws and regulations.

1.15.6.1.6
(02-26-2025)
**Acronyms/Terms/
Definitions**

- (1) The table lists commonly used acronyms and terms:

Acronym	Term
BU	Business Unit
BYOD	Bring Your Own Device
CFR	Code of Federal Regulations
DPO	Digitization Project Owner
DVA	Digitization Validation Assessment
ELC	Enterprise Life Cycle
ERA	Electronic Records Archives
ERM	Electronic Records Management
ERSA	Electronic Recordkeeping System Assessment
FACA	Federal Advisory Committee Act
FEDRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
FRC	Federal Records Center
GRS	General Records Schedules, Document 12829
IM	Instant Message
KM	Knowledge Management
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
OneSDLC	One Solution Delivery Lifecycle
PGLD	Privacy, Governmental Liaison and Disclosure
POCs	Points of Contact
PST	Personal Storage Files
QAC	Quality Assurance and Control
QC	Quality Control
RCS	Records Control Schedules, Document 12990
RIM	Records and Information Management

Acronym	Term
SDLC	Solution Development Lifecycle
SOP	Standard Operating Procedure(s)
USC	United States Code

- (2) The following terms and definitions apply to this IRM section:
- a. Records - all recorded information such as books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of form or characteristics, made or received by a federal agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. (44 USC 3301)
 - b. Non-records - work-related documents that do not qualify as records such as duplicate copies, convenience/reference copies, and stocks of publications.
 - c. Personal Materials - anything belonging to an individual that is not used to conduct agency business.

1.15.6.1.7
(02-26-2025)

Related Resources

- (1) The following table lists the primary sources of guidance on managing electronic records:

IRM	Title	Guidance on
IRM 1.10.3	Standards for Using Email	Standards for using email in the most effective and productive manner
IRM 2.31.1	One Solution Delivery Life Cycle Guidance (formerly IRM 2.16.1, Enterprise Life Cycle (ELC) Guidance - obsolete)	The delivery of IT systems and applications modernized at the IRS through a single software development life cycle approach and delivery model
IRM 10.5.1	Privacy Policy	IRS privacy policy
IRM 10.8.1	Policy and Guidance	The foundation to implement and manage security for information systems security within the IRS, including cybersecurity
IRM 10.8.26	Wireless and Mobile Device Security Policy	The minimum security controls required to safeguard government furnished and non-government furnished/personally owned mobile devices
IRM 10.10.1	IRS Electronic Signature (e-Signature) Program	The IRS policy on implementation and usage of e-Signatures
IRM 11.3.1	Introduction to Disclosure	The disclosure program and the legal authority for the program
IRM 25.3.1	General Guidelines	General information regarding suits that may be filed by or against the United States

(2) Employees will find the following information helpful:

- *Records and Information Management (RIM) SharePoint (including POCs)*
- *44 USC 3301, Definition of a record website*
- *OMB/NARA M-23-07, Update to Transition to Electronic Records*
- *OMB/NARA M-19-21, Transition to Electronic Records*
- *Document 12829, General Records Schedules (GRS)*
- *Document 12990, IRS Records Control Schedules (RCS)*
- *Is It a Record?* flowchart
- *System ERM Requirements*
- *Digitizing Federal Records*
- *Records Modernization Forms*
- IRS Records and Information Management Program office email at **Records Management* mailbox

1.15.6.2
(02-26-2025)
**Basic Electronic
Records Management
Definitions**

- (1) An electronic record contains information recorded in a form that is machine-readable (e.g., information that only a computer or similar system can process, and which, without a computer, would not be understandable to people). Recorded electronic information becomes a federal record when it satisfies the statutory definition of a “record,” and is the same definition applied to information recorded on paper. Basic definitions pertaining to electronic records management are:
- a. **Accessioning** - the process of sending permanent records to the National Archives and Records Administration (NARA), then NARA takes legal custody of the records and in most cases, takes physical custody of the records as well. Accessioned records become the property of NARA. *Accessioning* guidance and policy is found on NARA’s website.
 - b. **Analog Records** - term most often used as a synonym for paper records, but also includes records on microfilm as well as records stored on nondigital electronic tape, disc, or wire that are either eye-readable or do not contain digital data.
 - c. **Born Digital** - records which have been generated entirely electronically, e.g., a document created in a word processing application, as opposed to a scanned image of a paper document.
 - d. **Capstone** - a roles-based/account-based approach to (electronic) management of email records that allows for the capture of records that must be preserved as permanent from the accounts of officials at or near the top of an agency or an organizational subcomponent (i.e., Capstone officials). See *NARA Bulletin 2013-02* (Aug. 29, 2013).
 - e. **Collaboration Tools** - used to allow multiple users access to the same document for purposes of sharing information.
 - f. **Data File** - numeric, textual, or graphic information that is organized in a strictly-prescribed form and format.
 - g. **Database** - (in electronic records) - a set of data, consisting of at least one file or a group of integrated files, usually stored in one location and made available to several users at the same time for various applications.
 - h. **Database Management System** - a software system used to access and retrieve data stored in a database.
 - i. **Digitalization (also known as digital transformation)** - the process of converting text, pictures, or sound into a digital form that can be processed by a computer, easily shared, and accessed. It usually involves a comprehensive business process redesign and/or policy updates to reduce and/or eliminate paper. The digitalization process includes planning, assessing, preparing, digitizing, documenting metadata, running quality control (QC) checks, validating, storing, and managing the digitized records.

Example: End-to-end tax return processing that allows for access and all downstream (collections, examinations, audit, etc.) actions to be performed.
 - j. **Digitization** - the process of scanning original source documentation (see Original Source Record definition) in analog format (e.g., paper) to create an electronic version of the record; often used interchangeably with scanning, digital reformatting, digital imaging, and document conversion.
 - k. **Digitization Project** - any action a business unit (including an agent acting on the business unit’s behalf, such as a contractor) takes to reformat or convert records. For example, a digitization project can involve:

- A one-time effort to a multi-year digitization process,
 - Digitizing a single document to many boxes of records, and
 - Digitizing both active and inactive records.
- l. **Digitization Validation Assessment (Form 15408)** - the process used by the Records and Information Management (RIM) Program office within Privacy, Governmental Liaison and Disclosure (PGLD) to ensure digitization and validation standards have been met and align with IRS requirements (see Validation definition) before approval can be given to destroy the original source records (see Original Source Record definition) associated with the modernization project or initiative.
 - m. **Digitized Record** - an electronic record created by converting paper or other media formats to a digital form that is of sufficient authenticity, reliability, usability, and integrity to serve in place of the original source record (see Original Source Record definition).
 - n. **Disposition** - those actions taken regarding records no longer needed for current agency business and documented in the records control schedules (RCS).
 - o. **Disposition Authority** - the legal authorization for the retention and disposal of records.
 - p. **Document Conversion Services** - record digitization/conversion operations and projects related to document conversion; includes scanning of the original document's text and images, converting the information to digital data, transferring the data to a new media file, and formatting the information for use in a document imaging and storage system.
 - q. **Documentation** - records required to plan, develop, operate, maintain, and use electronic records. Included are system specifications, file specifications, codebooks, record layouts, user guides, and output specifications.
 - r. **Electronic Information System** - a system that provides access to computerized federal records and other information.
 - s. **Electronic Mail (email) Records** - records created or received on an electronic mail system including, but not limited to, correspondence among employees/colleagues containing briefing notes, policy decisions or reports for review, comment, or action; information requests from taxpayers requiring research, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.
 - t. **Electronic Mail (email) System** - a computer application used to create, receive, and transmit messages and other documents. **Exception:** Excluded from this definition are: file transfer utilities (software that transmits files between users but does not retain any transmission data); data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers; and word processing documents not transmitted on an email system.
 - u. **Electronic Messaging** - any method (systemic or human generated) used to create, transmit, communicate, or share information electronically. This encompasses emails, text messages, instant messages, social media messages, and other forms of electronic communication.
 - v. **Electronic Receipt** - information in email systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by addressee(s).
 - w. **Electronic Recordkeeping System** - a system where records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

- x. **Electronic Recordkeeping System Assessment (eRSA Form 15407)** - the process used by the RIM Program office within PGLD to ensure the repository aligns with the NARA requirements and establishes a risk assessment score for the system.
- y. **Electronic Records Storage Media** - material or platform used for the storage of electronic records.
- z. **Electronic Transmission Data** - information in email systems regarding the identities of the sender and addressee(s), and the date and time the messages were sent (sometimes referred to as metadata).
- aa. **Essential (Vital) Records** - records an agency needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the government and those affected by government activities (legal and financial rights records).
- ab. **Federal Information Security Modernization Act (FISMA)** - a framework of guidelines and security standards to protect government information and operations. FISMA was originally passed as the Federal Information Security Management Act in 2002 as part of the E-Government Act.
- ac. **Files Plan** - an office/organization tool for identifying records created/received within the organization, files arrangement, locations, transfer instructions, files retention and disposition instructions, and other specific instructions that provide guidance for effective management of records, including essential (formerly known as vital) records. IRS files plans can be found on the *RIM knowledge management site*. If you are unsure of the *file plan information* for your specific organization, please contact your *business unit information resource coordinators (BU/IRC)* or the *Records Specialist* assigned to your geographic location.
- ad. **Information Package** - the collection of all information included in the original source records (see Original Source Record definition) including contextual metadata, envelopes, handwritten notes, and attachments.
- ae. **Instant Messaging (IM)** - an electronic messaging service that allows users to determine whether a certain party is connected to the messaging system at the same time. IM allows users to exchange text messages with connected parties in real time. An example of an instant messaging system is Microsoft 365, a cloud-based communication and collaboration platform.
- af. **Itemized Audit Digitization Quality Review Sheet (Form 15408-A)** - the form is used by employees performing digitization QC and validation duties to verify and document that digitized records and associated metadata from one-time digitization project(s) or ongoing digitization operations comply with quality, accuracy, metadata, and usability digitization standards. Form 15408-A also allows employees performing digitization QC control and validation duties to document and report errors requiring remediation when detected.
- ag. **Metadata** - consists of preserved contextual information describing the history, tracking, and/or management of an electronic document.
- ah. **Migration** - act of moving records from one system to another (i.e., due to system shutdown and upgrade to new platform) while maintaining the record's authenticity, integrity, reliability, and usability.
- ai. **Official Business Record** - the final version of a record created and used for official business at the IRS (e.g., policies, briefings, reports, planning documents).

- aj. **Original Source Record** - the record or information from which a digitized version or digitized record is created - i.e., an original source record of a digitized Form 1120, U.S. Corporation Income Tax Return, is a paper Form 1120 mailed to the IRS by a corporation.
- ak. **Permanent Records** - documents that NARA appraised as having sufficient value to warrant continued preservation by the federal government as part of the National Archives of the United States. Permanent records are created or received while conducting government business. Examples of permanent records include organizational studies documenting changes in the way the IRS does business; advisory committee records; IRS press releases to the public; emails from the IRS Commissioner and other senior agency officials; and agency records classified as essential vital records, including FISMA essential vital records. A comprehensive listing of permanent records can be found in Document 12990, Records Control Schedules (RCS) 36, IRS Permanent Records Index.
- al. **Quality Assurance and Control (QAC)** - the process that verifies the quality, accuracy, and consistency of digitized (scanned) images to ensure the digitized records match the specifications outlined in 36 CFR 1236.46, Quality management requirements, as well as the standard operating procedures (SOP), project plans, and/or an approved Form 15408, Digitization Validation Assessment. The QAC review process is particularly important for scanning projects where paper records will be destroyed after scanning. The level of QAC varies based on the nature of the project, types of records, and materials being scanned. QAC helps the IRS ensure that the digitized versions are of suitable quality to replace original temporary source (e.g., paper) records as required by 36 Code of Federal Regulation (CFR) 1236.30-36, Digitizing Temporary Federal Records. The Form 15408-A, Itemized Audit Digitization Quality Review Sheet, within Form 15408, Digitization Validation Assessment, is used to document secondary QAC review results as a part of the digitization validation assessment (DVA) process.
- am. **Records Lifecycle** - the three basic stages federal records go through: creation (or receipt), maintenance and use, and disposition.
- an. **Records Management Application (RMA)** - software used to capture, categorize, locate, and identify records due for disposition, as well as store, retrieve, and document the disposition of records stored within its repository.
- ao. **Reformat/Convert** - a general term used to describe the process of changing the format of an original source record from analog to electronic.
- ap. **Retention** - the length of time a record must be kept (either in the office, in off-site storage or an approved electronic recordkeeping system) because it is needed for ongoing business, to document an action, or for statutory reasons.

Note: This is also referred to as a “retention period”.

- aq. **Risk Assessment** - in terms of records management, risk assessment is used to identify the risks to your records and information maintained in IRS repositories. It includes: Risk Identification and Risk Analysis.
- ar. **Risk Management** - the process of identifying (risk assessment) and evaluating (risk analysis) risk and then developing strategies to mitigate the risk.

- as. **Social Media** - internet or web-based technologies designed to disseminate information through social interaction. Examples include Facebook, X (formerly Twitter), Flickr, YouTube, and other such technologies.
- at. **Structured Electronic Data** - electronic data that resides in fixed fields within a record or file such as relational databases.
- au. **Target Repository** - electronic recordkeeping system that will store digitized records after digitization initiatives are completed.
- av. **Temporary Records** - records approved by NARA for disposal, either immediately or after a specified retention period outlined in Document 12990, RCS, and Document 12829, General Records Schedules (GRS). These records are sometimes called disposable or nonpermanent records.
- aw. **Text Message** - an electronic communication (aka Short Message Service, SMS) sent and received by a mobile phone or other similar device.
- ax. **Unstructured Data Record Content** - unstructured data that meets the criteria of a federal record as defined in 44 United States Code (USC) 3301.
- ay. **Unstructured Data Repository** - a digital system or directory primarily used to store or collaborate on unstructured data such as SharePoint. Such repositories might be equipped with out-of-the-box records management functionality.
- az. **Unstructured Electronic Data** - electronic data that does not reside in fixed fields, but is free-form text available in common office productivity tools such as word processors, spreadsheets, multimedia editors, presentations, diagrams, etc.
- ba. **Validation** - the process of ensuring digitized or digitalized information meets the technical and metadata standards required to use the information to replace the original source record as the authoritative record. Validation occurs when digitization is complete and must be conducted by staff that were not involved in the QC reviews conducted during the digitization process.

1.15.6.3
(03-27-2014)
**Responsibility for
Issuance of Guidance**

- (1) NARA is responsible for issuing standards for management of federal records created or received on electronic systems. These standards apply to all federal agency offices using office automation or information systems and will be followed by the IRS. The complete version of *36 CFR 1236*, Electronic Records Management, is available on the website.

1.15.6.4
(02-26-2025)
Electronic Records

- (1) An electronic record is any information that is recorded in a form that only a computer can process. Recorded electronic information becomes a federal record when it satisfies the statutory definition of a "record". This includes:
 - Records that are born digital,
 - Unstructured electronic data, and
 - Structured electronic data (i.e., relational databases).
- (2) Electronic records must be managed and protected against unauthorized access, use, alteration, alienation, or deletion until the authorized disposition date, regardless of whether they reside in the cloud; a contracted environment; or under the IRS's physical control.
- (3) Properly managing electronic records throughout their full lifecycle requires the combined efforts of RIM staff, Information Technology (IT) staff, and the program area staff responsible for the creation of the records and the system

(records repository). Electronic records are dependent on hardware, software, and media which change frequently. Rapidly changing technology puts the continued accessibility and usability of electronic records at risk if they are not managed effectively. IRS business units (BUs) must plan, budget, and implement mitigation strategies to counteract hardware and software dependencies of electronic records whenever the records and their associated metadata must be maintained and used beyond the planned life of the information system, media, or storage device in which the records are created, captured, or maintained. This will help to avoid records loss due to media decay or technology obsolescence.

1.15.6.5
(02-26-2025)
Metadata

- (1) Metadata consists of preserved contextual information describing the history, tracking, and/or management of an electronic document (36 CFR 1220.18). They describe context, content, and structure of electronic records and their management through time. Metadata describes the who, what, when, where, and why of the electronic records and is one of the core components of being able to easily locate those records when needed (e.g., data stamps). It can be used to identify, authenticate, and contextualize records as well as the people, processes and systems that create, manage, maintain, and use them. In general metadata is divided into one of three categories:
 - a. Descriptive metadata – describes a resource for purposes such as discovery and identification. Metadata in this area can include such elements as creator, file name, and description.
 - b. Structural metadata – indicates how objects are put together. It identifies file format type, hardware and software needed to render the data, and the compression method or encryption algorithms used, if any.
 - c. Administrative metadata – provides information to help manage a resource, such as when and how it was created, file format type and other technical information, and who can access it. It also includes rights management and preservation metadata.
- (2) Ensuring metadata is captured and maintained from the time records are created is essential for ensuring the authenticity, manageability, and usability of information over time. It is through complete, accurate, and consistent metadata that IRS BUs can successfully perform searches for materials in structured and unstructured electronic repositories. It is important to maintain persistent linkages between records and their associated metadata stamps. Once the record is captured in electronic information systems or unstructured electronic environments, the associated metadata (e.g., unique identifier, creator, date of creation) must be unaltered and complete, in compliance with a legal hold data call request. Similar to the electronic record, the associated record metadata must be managed and destroyed in accordance with the NARA-approved records control schedule. In addition, per *NARA Universal Electronic Records Management (ERM) Requirements*, electronic recordkeeping systems with metadata must include metadata tracking capabilities and reporting.
- (3) The metadata for records are details about documents/files or records series that describe or identify them and include:
 - The description of the content of the record,
 - The structure of the record (form, format, and relationships between record components),
 - The business context in which the record was created,

- The relationships with other records and metadata,
 - The identifiers and other information needed to retrieve the record, and
 - The business actions and events involving the record throughout its existence.
- (4) Electronic recordkeeping systems must define metadata to:
- Enable the identification and retrieval of records,
 - Associate records with changing business rules, policies, and mandates,
 - Associate records with agents, and their authorizations and rights with regards to the records,
 - Associate records with their business activities, and
 - Track processes carried out on records.
- (5) Permanent electronic records in electronic recordkeeping systems must include the following metadata elements:
- File Name,
 - File Description,
 - Creator,
 - Creation Date,
 - Unique Record Identifier,
 - Record Value (e.g., Permanent),
 - RCS/GRS Number,
 - Security/Access Restriction, and
 - Rights.
- (6) Metadata elements such as coverage and relation must also be provided if they apply to the records being transferred.
- (7) Temporary electronic records managed in electronic recordkeeping systems must include the following metadata elements:
- File Name,
 - File Description,
 - Creator,
 - Creation Date, and
 - Unique Record Identifier.
- (8) Metadata elements such as essential records status, security/access restriction, and rights must also be provided when applicable. For additional details regarding metadata requirements, please contact **Records Management* or visit the *PGLD-RIM eRSA SharePoint* to start an assessment on your electronic recordkeeping system.

1.15.6.6
(02-26-2025)
**Scheduling Electronic
Records**

- (1) A records schedule provides mandatory instructions for the disposition of records when they are no longer required by the agency. All IRS records, including records in electronic systems, must be scheduled with NARA (44 USC 3303). The records must be covered by an IRS-specific schedule (i.e., IRS records control schedule) or a general records schedule (GRS). Records disposition instructions for each IRS major function are published in Document 12990, RCS. Records disposition instructions used by the IRS and other federal agencies for most administrative recordkeeping requirements, are published in Document 12829, GRS. Records are not authorized for destruction without a NARA-approved schedule.

- (2) The IRS Records Officer is the liaison with NARA and customer organizations for ensuring that electronic records and the related documentation are scheduled with NARA and retained for as long as needed by the IRS. The IRS Records Officer is responsible for:
- Ensuring electronic records series, including master files data and related system documentation and indexes, are maintained in accordance with a NARA-approved disposition authority. The records and information in electronic information systems, including those operated for the IRS by a contractor, must be scheduled as soon as possible, and no later than one (1) year after system deployment.
 - Transferring permanent electronic records and related documentation and indexes to NARA in accordance with disposition instructions.
 - Providing guidance for the destruction or other disposal of temporary electronic records no longer having sufficient administrative, legal, research or other value warranting further retention.

Note: IRM 1.15.3, Disposing of Records, provides additional guidance on the IRS RCSs.

Note: All RCS dispositions must be reviewed and approved by the IRS Records Officer and NARA prior to IRS implementation and use. Therefore, IRS staff are reminded not to develop or revise records retention instructions for organizational and functional (i.e., program) operations without first consulting the Servicewide RIM Program office at **Records Management*.

1.15.6.7
(02-26-2025)
**Creation, Use, and
Maintenance of
Structured Electronic
Data**

- (1) In accordance with *36 CFR Chapter XII, Subchapter B, Office of Management and Budget (OMB) Circular A-130 par. 8a (k)*, and *NARA Universal Electronic Records Management (ERM) requirements*, records and information management requirements must be incorporated into the design, development, and implementation of electronic information systems that produce, use, or store official records and data files. In addition, all official IRS records in electronic recordkeeping systems must be scheduled (44 USC 3303) with NARA and covered by an IRS-specific RCS listed in Document 12990 , or covered by Document 12829 , GRS for records that are common to several or all agencies of the federal government.
- (2) The RIM Program office took the RIM-specific system requirements from the NARA universal ERM requirements, as well as the IRS RIM business rule-specific requirements, to create the PGLD-RIM System ERM Requirements, which can be found on the *RIM knowledge management (KM) ERM site*. These requirements need to be applied to the full lifecycle of records and must be used by system owners/managers when developing and updating official IRS electronic recordkeeping systems. IT and system owners/managers are responsible for ensuring that systems meet the PGLD-RIM System ERM requirements and IRS policy. Contact the RIM Program office at **Records Management* for requirements information.
- Acquisitions of Information and Technology Services must include RIM clauses and requirements in solicitations when procuring electronic information systems to manage or store official IRS records and information. See the IRS acquisition policy site for RIM contract clauses and the RIM KM site for *system ERM requirements*. NARA also provides basic recommendations for *RIM contract language*.

- b. IT Investment Design and Management must fully incorporate records and information management, retention and disposition requirements into information lifecycle processes and stages, including the design, development, implementation, and decommissioning of information systems, particularly internet resources to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service (OMB A-130, Managing Information as a Strategic Resource). The RIM Program office must participate in the SDLC and capital planning and investment control (CPIC) processes to ensure temporary and permanent electronic records are appropriately identified, scheduled, and stored in approved recordkeeping solutions. System owners and managers of new IT electronic recordkeeping solutions, including cloud services, must notify the RIM Program office via **Records Management* during the allocation phase of a project. In addition, Form 15407-A , One Solution Delivery Lifecycle (OneSDLC) Records and Information Management (RIM) Checklist, assists IRS project/system owners with integrating scheduling and system electronic records management (ERM) requirements into the OneSDLC pathway. The checklist identifies certain points in the SDLC process (allocation, readiness, and execution) to ensure that sound RIM practices are incorporated into the development of proposed IT solutions managing official IRS records. IRS project/system owners must use Form 15407-A as a part of the *OneSDLC* pathway when developing new electronic recordkeeping solutions.

Note: The Form 15407-A checklist cannot be used for waterfall methodologies.

- (3) Legacy/existing systems must be reviewed by the RIM Program office to ensure compliance with NARA's scheduling and electronic recordkeeping requirements. The Form 15407 , Electronic Recordkeeping System Assessment (eRSA), is the evaluation method used by RIM to assess if an electronic information system that produces, uses, or stores official IRS records is compliant with NARA's scheduling and electronic records management requirements. This form is required for system owners and/or managers managing official IRS records and information in electronic recordkeeping systems. Upon notification, system owners and/or managers of electronic recordkeeping systems must work with the RIM Program office to complete the form. Once an eRSA is completed, the RIM Program office generally will not have to reassess the system for three (3) years as long as no major/significant system/application/project changes have been made, no new uses to the system or application significantly change how the records are managed, or no new business processes resulting in new records or data being created are integrated into the system.

Note: Requirements in Form 15407 represent the baseline requirements with records management laws and regulations. System developers must contact General Counsel, eDiscovery, Privacy, Freedom of Information Act (FOIA), Disclosure, and Continuity of Operations program offices for requirements related to those areas.

- (4) In accordance with 36 CFR 1236.26(b) on the actions agencies must take to maintain electronic information systems, IT and IRS offices must maintain adequate and up-to-date technical documentation (e.g., data dictionaries, user guides, file specifications, code books, and record layouts) for each electronic information system that produces, uses, or stores data files.

- (5) Electronic system owners (subject to projects that follow the Enterprise Life Cycle (ELC) or OneSDLC process) must follow appropriate system retirement, decommissioning, and/or shutdown procedures when a system is scheduled for cancellation. Any records that have not yet met their required retention periods must be migrated to another approved recordkeeping system. When migrating records, all metadata must be preserved and accompanied with the transfer. The process is defined through the following series of actions to ensure orderly and efficient performance of essential shutdown activities.
 - a. If information is to be migrated to another system, you must:
 1. Notify the RIM Program office of changes to system (i.e., name change, changes in functionality),
 2. Determine if any changes need to be made to the disposition of the new system based on changes in functionality, and
 3. Manage the new system in accordance with an approved disposition authority.
 - b. If the information is not being migrated to a new system, you must:
 1. Notify the RIM Program office that this information will no longer be collected, and
 2. Establish a plan to manage any legacy record data that has not yet met its approved disposition.

1.15.6.8
(02-26-2025)
**Creation, Use, and
Maintenance of
Unstructured Electronic
Data**

- (1) **Records and Information Management Program Office Responsibilities**
 - a. **Records Management Controls** - All unstructured data recordkeeping systems or repositories managing official records must be configured appropriately according to the approved RCS or GRS. Specifically, this includes:
 1. Working with BUs to prepare, review, and approve requirements for any system or repository capable of storing unstructured data.
 2. Working with BUs on the association of unstructured data record content to an approved records control schedule and disposition instruction according to 36 CFR 1236.20(b)(3), Organize records.
 3. Providing guidance on the preservation of unstructured data record content for as long as needed to conduct agency business and meet NARA-approved dispositions according to 36 CFR 1236.20(b)(6), Preserve records.
 4. Providing guidance on the deletion of temporary records, and the transfer to NARA of permanent, unstructured data record content according to 36 CFR 1236.20(b)(7), Execute disposition.
 - b. **Automated Disposition Policies** - The RIM Program office is responsible for working with BUs to ensure the appropriate development, maintenance and publication of automated disposition policies, are in the unstructured data systems or repositories according to the respective NARA-approved records control schedules. Automated disposition policies are rules configured in unstructured data systems or repositories

to destroy or export records when criteria are met. Automated disposition rules which affect the destruction or export of unstructured data record content must be reviewed by the RIM Program office prior to configuration. This approval process must be built into unstructured data repositories to the highest extent possible.

- (2) **Information Technology (IT) Responsibilities** - IT must provide storage locations for unstructured data that meet requirements described under (1a-b) above. IT must ensure that the records management functionality is appropriately enabled in all applicable document management systems. This includes the ability to appropriately apply the NARA-approved records disposition authorities upon deployment of the system or repository.
- (3) **All employee responsibilities** - IRS employees **must** be able to distinguish between federal records and those non-record documents that may be business-related but do not meet the legal definition of a record (44 USC 3301) or warrant long-term retention. IRS employees **MUST** manage all information, both record and non-record, according to the guidance below.
 - a. **Document Management Systems/Collaboration Environments (such as Documentum, SharePoint, etc.)** - Document management systems and collaboration environments are appropriate platforms to store unstructured electronic records. The RIM Program office, system administrators, and content owners must coordinate to establish/identify appropriate dispositions for the content stored within these records storage locations. Automated disposition policies must be configured to manage information in these environments to the highest extent possible.
 - b. **File Shares (Shared Drives)** - These repositories do not currently provide the functionality necessary to electronically manage record information. Records (permanent and temporary) must be managed in accordance with the criteria listed in IRM 1.15.6.1, Program Scope and Objectives, or moved to a compliant document management system/collaboration environment. If either option is not possible, manual processes and procedures must be developed and a copy provided to the RIM Program office. Written procedures must include the following:
 - Ensuring records are covered by the NARA-approved dispositions.
 - Communicating those NARA-approved dispositions to the users of the file share so retention requirements are well understood.
 - Reviewing annually the file share to take disposition actions required by the NARA-approved schedule and document the action taken.
 - c. **Laptop/Desktop Hard Drives** - These storage locations do not provide the functionality necessary to electronically manage record information. Laptop/desktop hard drives must only be used to store personal materials, reference materials, or working papers that do not need to be accessed/collaborated on by others. All final recordkeeping copies must be moved to a compliant document management systemic/collaboration environment.
 - d. **Individual Employee Networking sites (OneDrive)** - Since OneDrive is not intended for long-term or permanent storage of federal records, a “7-year after last modified, then delete” retention has been applied by default to all OneDrive locations. For reference material needed longer than 7 years, a “10-year after last modified, then delete” label can be applied. Federal records can be stored temporarily in OneDrive until:

1. Any working papers that become federal records have been completed, and
2. A compliant recordkeeping location is identified/created (SharePoint or another electronic recordkeeping location).
- e. **Removable Media** - This type of media does not provide the functionality necessary to electronically manage record information. Media such as flash drives, CDs, DVDs, and removable storage drives can be used to transfer a record to an approved recordkeeping system or to back-up material saved to a hard drive.
- f. In all cases in which removable media is used, an inventory must be maintained. The removable media must be properly labeled, stored under proper environmental conditions, tested regularly to check for degradation, and protected from unauthorized access or modification. Removable media storage labels must include the BU/employee name, the applicable records control schedule on the media (particularly if used to store records, see Note below), the date range of the files, and the version of software application(s) used.

Note: The RIM Program office (records office) grants exceptions to this records storage policy as needed, based on suitable justification and a thorough assessment of evident and potential risks. For example, examination case closures that require storage of records on removable media due to software constraints or file size, generally are considered a policy exception (see IRM 4.10.9, Workpaper System and Case File Assembly, and IRM 4.33.1, Managing Electronic Records from Taxpayers and Third Parties). Contact the RIM Program office at **Records Management* to discuss the need for a policy exception.

- g. **Backups** - Employees are responsible for the backup of information saved to individual laptop/desktop hard drives to ensure data is not lost.

Note: Contact your Business Systems Planning (BSP) office for assistance with determining the best environment to store your information. For general guidance on the management of unstructured data, contact the RIM Program office at the **Records Management* mailbox.

1.15.6.9
(02-26-2025)
**Managing Electronic
Mail Records**

- (1) **IRS Role-based Approach** - In accordance with NARA's Capstone approach to email management, the IRS manages email records (by default) based on the role of the email account user and/or office. Email records are captured and managed according to the user role using the following retention approach:

Role	Position	Email Records Management
Senior Officials	<ul style="list-style-type: none"> Commissioner Deputy Commissioner Chief Counsel Advisors, and other top-level positions identified in the IRS Organizational Chart and in Capstone/NA Form 1005 Employees in “Acting” or “Detail” status to any of these positions 	<p>The IRS will retain permanent email records according to the approved email records schedule and then <i>accession</i> them into the National Archives of the United States.</p> <p>Note: The IRS Records and Information Management (RIM) Program office and the Information Technology (IT) office maintain the official list of Senior Officials’ email accounts.</p>
All other IRS employees		The IRS will retain according to the email records schedule, and delete when twenty (20) years old.

(2) **Exceptions:**

- a. **Email records associated with official recordkeeping files:** When business needs require email records to be retained with other records (such as part of an investigation, contract, project, or other case file), forward or copy these email records to the appropriate recordkeeping system (i.e., electronic recordkeeping system or paper file) for maintenance as part of official files according to Document 12990, RCS, or Document 12829, GRS. The Capstone, role-based approach does not replace existing business practices that require email messages and other related records to be retained together in established recordkeeping systems, which may be paper or electronic.

Note: GRS 5.1, item 020, Non-recordkeeping copies of electronic records, authorizes deletion of electronic email records once filed in an official recordkeeping system (such as with a related case file, or within another records management application).

- b. **Non-Records:** All account holders must delete non-records when no longer needed for reference. Non-records include non-business related messages, “broadcast” messages (e.g., IRS messages to all staff), and advertisements.
- c. **Personal Messages:** All account holders must delete personal messages to ensure separation from record email messages. Personal messages are those messages from family/friends or colleagues that do not have an effect on the conduct of agency business.
- d. **Short-term (Transitory) Messages:** All account holders must delete short-term (transitory) messages immediately or once final action is complete. Short-term (transitory) messages are those business-related messages such as routine exchanges of information, inquiries about availability and other routine actions.

1.15.6.9.1
(03-18-2021)

**Email Sent or Received
Using Organizational
Mailboxes**

(1) Use of Organizational Mailboxes:

- a. An organizational mailbox (or group email account) is a shared email account used to send and receive BU correspondence. A shared mailbox has an email address, storage quota, and can only be accessed by members of an authorized group.
- b. Organizational email accounts must only be used for sending or receiving email related to the specific organization's business purpose.
- c. Organizational mailboxes must not be used for personal communications (emails strictly personal in nature and not related to agency business), and if they are, they must be deleted immediately after close of the discussion thread.
- d. Capstone officials must not use organizational mailboxes for communications more appropriately reserved for their individual accounts.
- e. The organization or organizational component using a shared mailbox must designate a mailbox manager or "owner" (could be more than one person) with primary responsibility for the overall management of the mailbox. The mailbox owner must establish business use rules and ensure compliance with agency and organizational policy for assigning emails, tracking email responses, and preserving the emails as appropriate.
- f. Organizational mailboxes do not have archive mailboxes. An owner must create an archive folder in the organizational mailbox and move older messages there to keep the inbox current and clutter-free.

(2) Preservation:

- a. Organizational mailboxes, with few exceptions, are maintained as temporary twenty (20) year accounts.
- b. For an organizational mailbox account, preservation of record emails means preserving the final, comprehensive thread of incoming messages and outgoing responses of any communications that are initiated directly by the mailbox owner and/or staff monitoring the mailbox. Duplicate emails may be deleted.
- c. Preservation of the email record also means ensuring retention for situations where incoming emails are forwarded to other IRS staff (including staff outside the organization to which the mailbox is assigned) for a response based on subject matter expertise. The organizational mailbox record must preserve the incoming email and the outgoing email that provides documentation of the request, who is being asked to provide the response, and the response due date.
- d. The employee tasked to respond must ensure their follow-up actions are appropriately preserved. This role-based approach does not replace existing business practices that require email messages and other related records to be retained together in established recordkeeping systems and maintained per approved records retentions.

1.15.6.9.2
(03-18-2021)

**Federal Advisory
Committee Act (FACA)
Email Records**

(1) Use of Personal email to Conduct Federal Advisory Committee (FAC) Business:

- a. Email can be used for all informal and formal business communications and collaborations among FAC members, stakeholders, and/or agency committee staff (such as designated federal officer, DFO).

- b. IRS FAC members are not issued irs.gov email accounts to conduct FAC business. Use of employer-sponsored email accounts or personal email accounts for FAC-related work is permitted and expected.

(2) Preserving Record Email Exchanges (FAC Members):

- a. To ensure compliance with records management/retention requirements located in Document 12829, GRS 6.2, Federal Advisory Committee (FACA) Records, all IRS FAC members must copy a designated committee organizational mailbox address for all substantive FAC-specific business emails.
- b. To ensure substantive records created by committee members include correspondence documenting decisions, discussions, or actions relating to the work of the committee, including email, exchanged between one or more committee members and/or agency committee staff (such as the DFO).
- c. To exclude from this sub-set of substantive (permanent) committee member communications, records relating to purely logistical or administrative aspects of committee activities, such as meeting planning (e.g., location, administrative issues and other meeting arrangements). These records (including emails) can be deleted when no longer needed, and do not require copying the committee mailbox. However, if committee member email contains a mix of administrative and substantive FAC business, the email must be preserved.

(3) Designated Federal Officer (DFO) Recordkeeping Responsibilities:

- a. The DFO maintains the official records an advisory committee creates or receives (see *41 CFR 102-3.175*, What are the reporting and recordkeeping requirements for an advisory committee). This includes correspondence between committee members and other records that relate to the committee's decisions or actions (see Document 12829, GRS 6.2, Federal Advisory Committee Records).
- b. The DFO (or other designated committee official) must assume primary responsibility for overall management of the FAC mailbox.
- c. Permanent records generated by or for an advisory committee must be transferred to NARA when records are fifteen (15) years old or upon termination of the committee, whichever is sooner. The records must be processed in accordance with the Federal Records Act (FRA), 44 USC Chapters 21, 29, 31, and 33, and regulations issued by NARA. [41 CFR 102-3.175(e) Advisory committee records]

1.15.6.9.3
(02-26-2025)
**Email Sent or Received
Using Government-
issued Communications
Tools**

- (1) Business-related emails sent or received on government-issued devices such as cell phones, smart phones, etc. will be managed as part of the IRS Exchange Server email environment in accordance with the account-based email policies set forth in the previous subsections.

1.15.6.9.4
(02-26-2025)

**Email Created Using
Personal or Non-IRS
Communications Tools
(Bring Your Own Device
(BYOD) Program)**

- (1) Business-related emails sent or received as part of the bring your own device (BYOD) program will be managed in accordance with the account-based email policies set forth in previous subsections. Refer to IRM 10.8.26, Wireless and Mobile Device Security Policy (formerly Government Furnished and Personally Owned Mobile Device Security Policy).

Note: The Protecting Americans from Tax Hikes (PATH) Act of 2015, Section 402, IRS Employees Prohibited from Using Personal Email Accounts for Official Business, states that “No officer or employee of the Internal Revenue Service may use a personal email account to conduct any official business of the government”. Refer to IRM 10.5.1.6.8.4, Emails with Personal Accounts, for guidance.

1.15.6.9.5
(03-18-2021)

**Email Created Using
Personal or Non-IRS
Communications Tools
(not part of the BYOD
Program)**

- (1) In accordance with IRM 10.8.1, Policy and Guidance, and IRM 10.5.1, Privacy Policy, IRS employees are prohibited from using personal, or non-IRS, email and other communication tools to conduct IRS business, except in emergency situations.

- a. Business-related communications must be copied to the employee’s official email account at the time of transmission of the email.
- b. Maintain business-related communications in accordance with the appropriate records management policies.
- c. Copies left behind on personal devices must be appropriately managed and deleted in a timely manner after they are saved in a compliant recordkeeping system. All government-owned information is subject to discovery and FOIA.

1.15.6.9.6
(11-23-2016)

Encrypted Email

- (1) The RIM Program office will provide oversight for the following:

- For email accounts containing permanent email, work with the appropriate BU functions to ensure that encrypted emails are unencrypted prior to transfer to NARA. This includes deactivation of passwords or other forms of file level encryption that would impede access to record data.
- When transferring permanent records to NARA, RIM will ensure that any restrictions on the use and examination of records, such as those under IRC 6103 and the FOIA are included in documentation accompanying the transfer.

1.15.6.9.7
(03-18-2021)

Litigation Holds

- (1) For email accounts subject to litigation holds, (see IRM 25.3.1, General Guidelines and *Chief Counsel Directive Manual (CCDM) 34.7.1.1.4*, Discovery Obligations to Preserve Evidence, Including Electronically Stored Information (ESI)), potentially relevant email or instant messages cannot be deleted or altered while the litigation hold is in effect. If account holders are separating from the IRS, and their information is under a litigation hold, they **must** notify the Chief Counsel Attorney who issued the hold, and they **must** notify their managers who **must** ensure that upon separation, all information is maintained and accessible until the litigation hold is lifted. This includes ensuring that ESI on separating employees’ laptop or other personal computer equipment is preserved, and not erased by IT personnel. For further information on separating employee guidance, see IRM 1.15.5, Relocating/Removing Records.

- (2) Email or instant messages may be subject to other holds, such as in connection with congressional inquiries and FOIA requests, and procedures in which the preceding paragraph will apply.

1.15.6.9.8
(03-18-2021)
System Backups

- (1) Email backup systems and media do not provide the appropriate recordkeeping functionalities and must not be used as the IRS electronic recordkeeping system.
- (2) Backup systems must adhere to prescribed management requirements as defined in Document 12829, GRS 3.2 item 040, System backups and tape library records, and item 050, Backups of master files and databases.

1.15.6.10
(02-26-2025)
**Judicial Use of
Electronic Records**

- (1) Electronic records are admissible as evidence for use in court proceedings, as set forth by the Federal Rules of Evidence. This is accomplished by thoroughly documenting the recordkeeping system's operation and any associated controls imposed upon it to maintain system and record integrity. IRS offices must implement the following procedures to enhance the legal admissibility of electronic records:
 - a. Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach,
 - b. Verify that security and audit procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions,
 - c. Identify the electronic media on which records are stored throughout their lifecycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records, and
 - d. Coordinate all the above with the Office of Chief Counsel, the IRS Records Officer, and senior records management staff.
- (2) Digitized records must be reviewed for completeness and accuracy and stored in authorized electronic recordkeeping systems that can successfully manage, safeguard, and produce the records throughout their lifecycle in accordance with federal laws and regulations.

1.15.6.11
(02-26-2025)
**Security of Electronic
Records**

- (1) IT and IRS offices with responsibility for electronic records must implement and maintain an effective records security program that incorporates the following:
 - a. Ensures that only authorized personnel have access to electronic records.
 - b. Provides for backup and recovery of records to protect against information loss or corruption.
 - c. Ensures that appropriate IRS personnel are trained to safeguard sensitive or classified electronic records. Classified electronic records must be stored on approved systems located inside a certified security area and accessed by authorized holders. See IRM 10.9.1, Classified National Security Information (CNSI).
 - d. Minimizes the risk of unauthorized alteration or erasure of electronic records.
 - e. Provides protection for electronic records that are restricted from disclosure by the Privacy Act, the Federal Information Security Modernization Act (FISMA), the Computer Security Act, and other statutes, regulations, executive orders, or authorities.

- f. Protects federal information that is collected, maintained, processed, disseminated, or disposed of by cloud service offerings, in accordance with Federal Risk and Authorization Management Program (FedRAMP) requirements.
- g. Protects sensitive but unclassified (SBU) data in accordance with any safeguarding guidelines from the originator(s) of the material, IRS policy, and/or applicable statutes. Refer to IRM 10.5.1.2.2, Sensitive But Unclassified (SBU) Data, for additional guidance.

1.15.6.12
(02-26-2025)

Disposition of Electronic Records

- (1) Disposition is the third and final stage of the lifecycle of electronic records. Disposition refers to the actions taken regarding IRS records after they are no longer needed to conduct current IRS business. NARA authorizes either the disposal of records or transfer of records to the National Archives for preservation and research. Disposition actions of electronic records include:
 - a. Transfer of records from the IRS to another federal agency.
 - b. Transfer of permanent records to NARA.
 - c. Disposal of temporary records no longer needed to conduct IRS business, usually by destruction or occasionally by donation (or transfer to another agency).
- (2) Refer to IRM 10.5.1.6.10.2, Electronic Disposition and Destruction, for additional disposition guidance.

1.15.6.13
(02-26-2025)

Transfer of Permanent Records to NARA

- (1) The legal requirements for the transfer of permanent records to NARA are documented in *36 CFR 1235*, Transfer of Records to the National Archives of the United States, and set forth in general form in the subsections below. If you need additional guidance after confirming your records retention and disposition authority, consult the IRS RIM Program office or your *BU/IRC* for more detailed instructions and guidance on the transfer of permanent IRS records.

1.15.6.13.1
(02-26-2025)

Transfer Forms for Permanent Records

- (1) Permanent records, hard copy (analog) and electronic, are transferred to NARA in accordance with a completed Transfer Request (TR) via the Electronic Records Archives (ERA).
- (2) Contact your *Records Specialist* or contact the RIM Program office at **Records Management* for instructions and assistance in providing required information and identifying other documents necessary for the transfer of permanent records.
- (3) Submit the required documentation through your *Records Specialist* to the IRS RIM Program office for completion, approval, and submission to NARA.
- (4) The NARA Bulletin 2015-04, Metadata Guidance for the Transfer of Permanent Electronic Records, defines the minimum set of metadata elements that must accompany transfers of permanent electronic records to the National Archives. Federal agencies are required to transfer documentation adequate for NARA to identify, service, and interpret permanent electronic records for as long as they are needed. Permanent records transfers to NARA must include the following metadata elements:
 - File Name,
 - Record ID,
 - Title,

- Description,
- Creator,
- Creation Date, and
- Rights.

- (5) Metadata elements such as coverage and relation must also be provided if they apply to the records being transferred. When transferring permanent records to NARA, IRS BUs must provide the metadata elements as an index in a machine-readable CSV file. The IRS must notify NARA if there are additional metadata provided with the transferred permanent records.

1.15.6.13.2
(03-18-2021)
**Transfer Documentation
for Permanent Records**

- (1) Federal agencies are required to transfer documentation adequate for NARA to identify, service, and interpret permanent electronic records for as long as they are needed (per 36 CFR 1235.48, What documentation must agencies transfer with electronic records?). Examples of documentation include records required to plan, develop, operate, maintain, and use electronic records and software, including, but not limited to, systems specifications, file specifications, codebooks, record layouts, user guides, and output specifications.
- (2) IRS offices must provide adequate technical documentation for each permanent electronic file identified for transfer to NARA to allow the records to be interpreted and understood in context. The extent, format, and content of the documentation varies for different types of electronic records. The documentation for a text file differs from the documentation for survey data, statistical files, indices, or tracking files. Within the types of records, documentation can vary as well. One survey might have very different documentation than another survey. This subsection provides some guidance to IRS offices regarding the content and potential sources of adequate documentation for permanent electronic records.

1.15.6.13.2.1
(03-18-2021)
**Sources of the
Documentation**

- (1) Sources of documentation exist in publications, administrative reports, annual reports, memoranda, user notes, system guides, inventories or control systems for electronic records, file descriptions, Privacy Act notices, or manual or automated data dictionaries. Some IRS records control schedules contain specific instructions concerning documentation that must accompany the transfer of electronic records. In general, technical requirements for hardware, software, and media, and requirements for metadata and contextual information are needed.

1.15.6.13.2.2
(03-18-2021)
**Format of the
Documentation**

- (1) Some of the documentation for electronic records may only exist in paper form and must be digitized in order to transfer the documentation to NARA. When the documentation is in electronic format, identify and transfer the documentation data as separate files along with the files containing the electronic records. The transfer format standards for electronic records also apply to documentation files. Microform copies of documentation, when available, are also useful.

1.15.6.13.2.3
(03-18-2021)
**Scope of the
Documentation**

- (1) Definitions:
- a. Content - that which conveys information (e.g., text, data, symbols, numerals, images, and sound).

- b. Structure - appearance and arrangement of the content (e.g., relationships between fields, entities, language, style, fonts, page and paragraph breaks, links and other editorial devices).
 - c. Context - background information that enhances the understanding of technical and business environments to which the records relate (e.g., metadata, application software, logical business models) and the origin (e.g., address, title, link to function or activity, agency, program or section).
- (2) The scope of the documentation consists of technical specifications, information about file content and structure, and context. Provided below is more information on each type:
- a. Maintaining content, structure and context of electronic records is vital. In order for records to serve as evidence, these three essential characteristics must be maintained. Whenever one of the characteristics is altered, the ability of records to accurately reflect the activities of an agency is diminished.
 - b. Each file requires a specific definition of its structure and content. This includes a record layout and a codebook for each field containing coded information. Documentation may be in data dictionaries, file, user, codebooks, or system manuals.
 - c. Contextual information explains how the electronic records fit into the IRS programs or mission. This information answers the questions: "Who created the Records?", "Why?", and "For What Purpose?"
 - d. If several data files containing related information are transferred, the documentation must include a description or diagram of how the files relate to each other. At a minimum, the documentation must specify the key fields, including primary keys, used to uniquely identify each record in a file, and the foreign keys, which relate records in one file to records in another file.

1.15.6.13.3
(03-18-2021)

**Transfer Formats for
Permanent Records**

- (1) NARA determines which sustainable formats are acceptable for transfer. NARA identified *preferred and acceptable file formats* for each category. IRS BUs must submit electronic records in files that are valid both according to the wrapper and any specified *codec* standards.
- (2) Records must be in a format that are not dependent on specific hardware or software, written in American Standard Code for Information Interchange (ASCII) or Extended Binary Coded Decimal Interchange Code (EBCDIC) with all extraneous characters removed (except records length indicators for variable length records, marks delimiting a data element, field, record or file, or standard generalized markup language (SGML) tags). Records will not be compressed unless NARA has approved the transfer in the compressed form in advance. If the records are in ASCII, the electronic files must have standard American National Standards Institute (ANSI) labels as specified in Federal Information Processing Standard (FIPS) Publication 79 and/or International Standards Organization (ISO) Standard 9600. If the records are in EBCDIC, the electronic files will have standard IBM OS or DOS labels.
- (3) Data files and databases must be transferred as flat files or as rectangular tables, that is, as two-dimensional arrays, lists, or tables. All records in a database or elements in a relational database must have the same logical format. Each data element within a record must contain only one data value. A record must not contain nested repeating groups of data items.

- (4) Textual documents in electronic form must be transferred as plain ASCII files; such files may contain SGML or extensive markup language (XML) tags.
- (5) Electronic mail, scanned images of textual records, portable document format (PDF) records, digital photographic records, web content records, and digital spatial data files must be transferred to NARA in accordance with requirements available on *NARA's website*.

1.15.6.13.4
(03-18-2021)
**Transfer Media for
Permanent Records**

- (1) When transferring permanent records to NARA, IRS offices must transfer electronic records on magnetic tape, compact disk-read only memory (CD-ROM), digital versatile disc-read only memory (DVD-ROM), external hard drive, or via secure FTP.

1.15.6.13.4.1
(03-18-2021)
Magnetic Tape

- (1) IRS offices can transfer electronic records to NARA on magnetic tape using either open-reel magnetic tape or tape cartridges. Open-reel tape must be on $\frac{1}{2}$ inch 9-track tape reels recorded at 1600 or 6250 bytes per inch. Tape cartridges must be 18-track 3480-class cartridges recorded at 37,871 bpi. Digital linear tape (DLT) IV cartridges must conform to the standards cited in the table listed in 36 CFR 1235.46 (What electronic media may be used for transferring records to the National Archives of the United States?). Regardless of the type of tape used, the data must be blocked at no more than 32,760 bytes per block

1.15.6.13.4.2
(03-18-2021)
**Compact Disk, Read
Only Memory (CD-ROM)
and Digital Video Disk
(DVD)**

- (1) The CD-ROM may contain software files and temporary records, but permanent records must be in files that contain only permanent records. CD-ROMs can be used as transfer media for fielded data files or text files if they:
 - a. Conform to the ISO 9660 standard and to the ASCII standard;
 - b. Are not compressed unless NARA has approved the transfer of the compressed form in advance; and
 - c. Are individually addressable.
- (2) DVDs can be used to transfer certain types of permanent files. It is recommended to look for gold or silver colored DVDs for the best quality. If transferring records that have been copied to a DVD from another media, agencies must transfer the premaster videotape and two copies of the discs. All permanent files must be on one DVD and not mixed with temporary files.

1.15.6.13.4.3
(02-26-2025)
**File Transfer Protocol
(FTP)**

- (1) The IRS can use FTP to transfer permanent electronic records to NARA, with approval from the IRS Records Officer and NARA. Each transfer of electronic records via FTP must be preceded by a NARA-approved Transfer Request (TR) or sent to NARA with the help of the RIM Program office.
- (2) FTP file structure may use the 64-character Joliet extension naming convention only when letters, numbers, dashes (-), and underscores (_) are used in the file and/or directory names, with a slash (/) used to indicate directory structures. Otherwise, FTP file structure must conform to an 8.3 file naming convention and file directory structure as cited in ANSI/NISO/ISO 9660 (incorporated by reference, see 36 CFR 1235.4, What publications are incorporated by reference in this part?). Permanent electronic records must be transferred in discrete files, separate from temporary files. All permanent records must be transferred in files that contain only permanent records.

1.15.6.13.4.4
(02-26-2025)

**Electronic Storage
Media Maintenance
Requirements for
Permanent Records**

- (1) The requirements for the maintenance of electronic records storage media for permanent records are documented in 36 CFR 1236.28, (What additional requirements apply to the selection and maintenance of electronic records storage media for permanent records?). Storage media must be assessed and tested regularly to check for degradation, and information must be transferred to new storage media before loss of quality or technological obsolescence occurs. If there is evidence of file corruption, data must be migrated to new media.
- (2) IRS BUs must maintain areas with electronic records storage media containing permanent and unscheduled records (e.g., records that are not covered by a NARA-approved records schedule) within the following temperature and relative humidity ranges: (a) Temperature - 62° to 68° F and (b) Relative humidity - 35% to 45%.

Note: In addition, IRS BUs must adhere to the media manufacturer's recommendations for specific environmental conditions in which the media must be stored.

- (3) IRS BUs must ensure that electronic records are not lost because of changing technology, portability of the medium (e.g., magnetic tape to CD-ROM), or through deterioration. Metadata must be maintained during transfers and migrations. The IRS must retain a copy of all permanent electronic records transferred to NARA until receiving official notification that NARA has accepted legal custody of the records.
 - a. If magnetic computer tape is used for permanent records, IRS BUs must annually read a statistical sample of all magnetic computer tape media containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss using the sampling measures in 36 CFR 1236.28 (e). Before the media is ten (10) years old, IRS BUs must copy permanent or unscheduled data on magnetic records storage onto tested and verified new electronic media. Once the new media has been sampled to assure the quality of the transfer, the original media can be destroyed with approval from the IRS RIM Program office. The IRS BUs must document when and how records are transferred from one storage medium to another.
- (4) Whatever media is used to store data is clearly labeled with enough information that its contents can be determined (e.g., optical media must have a physical label; data stored on a server must be indexed). IRS BUs must externally label the offline media with a brief description of the content, software application and versions used, date range of files, and date when then content was transferred to the medium. It is also recommended that an internal label such as an ASCII "read me" text file be included in case the external label becomes separated from the media.

1.15.6.14
(02-26-2025)

**Disposal of Temporary
Electronic Records**

- (1) Electronic records must be disposed of in a manner that protects any sensitive, proprietary, or national security information.
- (2) Temporary electronic records must be destroyed in accordance with the RCS or GRS. If a litigation hold or other disposal suspension activity is issued, any routine, approved destruction of effected records must cease immediately. Records destruction will not resume until a revocation order lifts the hold. Once the hold is lifted, the approved records disposition/destruction can continue.

IRS BUs must retain records approved for destruction beyond the period outlined in the records schedule if the records in question pertain to a court order, executive order, law, or approved business justification. Once the circumstances pertaining to the extended retention of records are no longer applicable, the IRS BUs must destroy the records in accordance with the records schedule.

- (3) There is no requirement to print born-digital or digitized source records for storage in FRCs. Source records are the original versions (e.g., paper, microfilm/microfiche) from which a digitized record is created. Born-digital and digitized source records must be (with no exception):
 - A full representation of the activities of the agency and can be depended upon for business transactions,
 - Protected against unauthorized alteration or deletion,
 - Accessible, retrievable, and usable by anyone who needs access for their full NARA-approved retention period, and
 - Stored in an electronic recordkeeping system or application that is evaluated via the RIM Form 15407, Electronic Recordkeeping System Assessment (eRSA), and/or Form 15408, Digitization Validation Assessment, when applicable.

Source records that have been digitized and meet the criteria in the above bullet list, can be destroyed in accordance with their record control schedule, unless there is a specific legal or regulatory requirement for the continued maintenance of the original versions (e.g., paper, microfilm/microfiche).

Note: If a longer retention need for the records is ongoing, please contact the RIM Program office to request a disposition update to the records schedule.

1.15.6.15 (03-18-2021) Use of Social Media

- (1) The IRS must manage record material produced or posted using social media such as Facebook, YouTube, X (formerly Twitter), Instagram, and other similar technologies.
- (2) The following records management considerations must be addressed with the use of these technologies:
 - a. The IRS must capture and manage information that meets the statutory definition of a federal record (44 USC 3301) in accordance with an approved RCS.
 - b. More than one office/agency may have a responsibility for the same records, depending on their use.
 - c. Records must be managed in accordance with the content and not the format.
 - d. Records determined to have permanent value must be transferred to NARA in an approved format. Records may have to be migrated from the original format to one accepted by NARA at the time of transfer.
- (3) For additional information and guidance, contact the IRS RIM Program office via **Records Management*.

1.15.6.16
(02-26-2025)

**Use of Collaboration
Tools**

- (1) The IRS must ensure the proper management of record materials produced using collaboration tools; this includes collaboration tools with multiple functionalities that interact together. Collaboration happens in multiple contexts, such as person to person, office to office, agency to agency, public to agency, or agency to public.
- (2) The following records management considerations must be addressed with the use of these technologies, which includes instant messaging, meeting chats, recorded meetings, transcripts, files sharing, etc.:
 - a. Information that meets the statutory definition of a federal record (44 USC 3301) must be captured and managed in accordance with NARA-approved Document 12990, RCS, or Document 12829, GRS.
 - b. Content created and stored in collaboration tools must adhere to the general rules for the privacy, security, transmission, and handling of sensitive but unclassified (SBU) information and personally identifiable information (PII) contained in IRM 10.5.1 , Privacy Policy and IRM 10.8.1 , Policy and Guidance.
 - c. Content created in collaboration tools that does not automatically capture instant messages, meeting chats, recorded meetings, transcripts, files, and metadata that meets the definition of a federal record, must be manually saved and stored in a recordkeeping environment that meets the requirements found in IRM 1.15.6.7 and IRM 1.15.6.8.
 - d. Content created using collaboration tools may be subject to litigation holds. Any content that is subject to a litigation hold must be preserved as directed by the Office of Chief Counsel (e.g., protected from deletion or used for the duration of the litigation hold and pending official "hold release notice" from Counsel).
 - e. Content created using collaboration tools may also be subject to other holds, such as those in connection with congressional inquiries, FOIA requests, audits, and NARA data calls. Any content subject to such holds must be preserved as directed by the business operating division (BOD) that is responsible for the matter.
 - f. IT will ensure all IRS collaboration tools or systems (including electronic messaging/instant messaging (IM), file sharing, etc.) adhere to the ERM requirements and regulations. If the collaboration tools do not have features that allow for records management compliance, IT must coordinate with the RIM Program office to develop methods that comply with the requirements below:
 - 1) IRM 1.15.6.1, Program Scope and Objectives - Requirements for all IRS electronic information systems and unstructured data repositories
 - 2) IRM 1.15.6.7, Creation, Use, and Maintenance of Structured Electronic Data
 - 3) IRM 1.15.6.8, Creation, Use, and Maintenance of Unstructured Electronic Data
 - 4) IRM 1.15.6.11, Security of Electronic Records
 - 5) IRM 1.15.6.14, Disposal of Temporary Electronic Records
 - 6) *NARA Universal Electronic Records Management system requirements*

- g. Contact the RIM Program office via **Records Management* for assistance with setting up proper electronic records management retention policy for new electronic recordkeeping databases and collaboration sites to ensure IRS records management policy and safeguards are incorporated and compliant.

1.15.6.16.1
(02-26-2025)
**Agency-approved
Electronic Messaging**

- (1) Short one-way, event-driven, or time-based messages (i.e., auto-response messages), facilitated by messaging services and sent to one or more individuals, are transitory records. These messages may be automated, system generated, or user initiated. There are two criteria for identifying a transitory record (Document 12829 , GRS 5.2, Item 010):
 - The records are required for only a short time (generally less than 180 days), and
 - The IRS does not require records to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making.
- (2) Both criteria must be met for the record to be transitory. System owners utilizing services that create messages that meet the definition of transitory, must ensure the originating system has the ability to maintain a record of the message for at least 180 days. Examples of electronic messages that are not appropriate for business use and not transitory (require preservation for a greater length of time), include those that:
 - Contain information that is necessary to document the activities and functions of the IRS adequately and properly.
 - Provide documentation of IRS decisions and commitments reached orally (person-to-person, phone, video, or in conference).
 - Convey information of value on IRS activities if the electronic mail message adds to a proper understanding of IRS operations and responsibilities.
 - Document the formulation and execution of policies and decisions.
 - Denote actions or decisions taken by IRS Capstone officials (senior agency employees) and non-Capstone officials/employees.
 - Provide evidence related to fiscal or legal rights and obligations.
- (3) The RIM Program office must review and approve system-generated message content to ensure messages are transitory in nature. For questions and approval, email **Records Management*.
- (4) Text messages created on mobile devices or cellular phones are prohibited, except in emergency situations. In the event of an emergency, users must document the information communicated as records and transfer to an IRS recordkeeping system/storage location within twenty (20) days (per the Federal Records Act, 44 USC 2911). This may be accomplished by copying the text message into a government-provided email account and then transferring to an IRS recordkeeping system/storage location with related records. Delete copies remaining on devices immediately after the record has been incorporated into the IRS recordkeeping system/storage location. All government-owned information is subject to discovery and FOIA.
- (5) All text messages must follow appropriate records retention requirements, as well as IT Security Policy in IRM 10.8.1.4.1.18.1 , Telecommunication Devices and IRM 10.5.1 , Privacy Policy.

1.15.6.17
(02-26-2025)
**Digitization
Requirements**

- (1) IRS BUs must contact the RIM Program office via **Records Management* prior to the start of digitization projects to ensure the technical, metadata, QC, and other digitization standards are appropriate for the source records being scanned. This requirement is essential for digitizing permanent records and long-term temporary records.
- (2) IRS employees digitizing small amounts of official records (e.g., one or two case files or travel receipts) on an ad hoc basis (e.g., every month) using a local approved scanner, do not have to complete the DVA process if they follow BU digitization standard operating procedure/job aid and store the digitized records in a repository approved by the BU.
- (3) All new digitization (scanning) contracts and service agreements for digitizing paper or other analog records must include the minimum IRS technical, metadata, and QC scanning requirements (see the *Minimum Digitization Requirements tables* on the RIM KM site for more details). In addition to specific business needs, the RIM Program office recommends that all new IRS digitization (scanning) contracts and service agreements use the *Digitization Contract and Service Agreements Requirements Checklist* found on the RIM KM site to ensure requirements are built into the digitization project lifecycle process. IRS BUs must refer to the employee toolkit in Document 13056 , Shipping Procedures for Personally Identifiable Information (PII), and refer to Document 13144 , Proper PII Shipping Procedures, along with IRM 10.5.1.6.9.3 , Shipping through Private Delivery Carrier, for additional information about the IRS policy for shipping PII.
- (4) Legacy scanning operations are also expected to produce readable images and address gaps in the minimum requirements through opportunities for improvement when available. These operations are strongly encouraged to evaluate and compare this guidance to their current practices and adopt the procedures (immediately or in a phased approach), but only if doing so does not jeopardize the status of their established standard business practice(s). Legacy scanning operations must contact RIM via **Records Management* to review digitization procedures to ensure compliance with 36 CFR 1236 requirements.
- (5) When planning to digitize official IRS records and information, digitization project and operations owners and managers must take into consideration records retention requirements, file format standards (e.g., PDF/A-1, TIFF), content image standards (e.g., resolution, color, skew), output information standards (e.g., OCR, metadata indexing), quality standards, hardware/software standards, disposal standards for original source records, storage requirements for digitized materials, and waiver process (if applicable). These considerations are key to being able to make appropriate and cost-effective decisions in digitization projects. Disposal of original source records associated with modernization projects or initiatives cannot be done until the RIM Program office has conducted assessments of the repository used to store the digitized record materials.
- (6) IRS BUs must develop and use a standard operating procedure (SOP), job aid, and/or project plan for digitization projects and operations. This requirement will ensure stakeholders are provided with guidance throughout the project (i.e., planning, document receipt and acceptance, document preparation, scanning/digital capture, technical and metadata standards, QC/review of scanned images, indexing, QC/review of indexing, document storage, and document delivery to the IRS).

- (7) Digitization project owners (DPOs) must use the QC Form 15408-A, Itemized Audit Digitization Quality Review Sheet, embedded within Form 15408, Digitization Validation Assessment, to document that all QC standards have been met in accordance with 36 CFR 1236 requirements.
- (8) DPOs must complete and submit Form 15408 to **Records Management* when digitized versions will replace the original source records as the “official record” or “recordkeeping copy”. Form 15408 is used to validate that the scheduling, technical specifications, metadata, QC, repository, and legal constraint requirements have been met before approval can be given to destroy the original source records associated with the modernization project or initiative.
- (9) Digitized records and their associated metadata must be validated and stored in electronic recordkeeping systems that can successfully manage, safeguard, and produce the records throughout their lifecycle in accordance with federal laws and regulations. DPOs will need to work with IT to identify an appropriate electronic recordkeeping system or repository to store the digitized records.
- (10) Once PGLD-RIM approves Form 15408 for ongoing digitization operations, Form 15408-A can be used to document QC and validation reviews for up to three (3) years. DPOs must maintain Form 15408-A with the approved Form 15408 for the records’ lifecycle.

Note: If the designated electronic recordkeeping system (repository) does not have both a completed Form 15407 and Form 15408, please contact PGLD-RIM via **Records Management* for immediate scheduling.

- (11) Form 15408 is not required if original source materials (e.g., paper) being digitized through digitization projects or operations do not meet the definition of a federal record, are a non-record, or a convenience or reference copy.

Note: Separate personnel staff must conduct the validation, independent from the staff that performed the digitization QC review described above in (6) of this subsection.

- (12) If Form 15407, Electronic Recordkeeping System Assessment (eRSA), is not completed on the electronic recordkeeping system or repository, then system owners and/or managers will need to complete an eRSA before original source records can be destroyed. See IRM 1.15.6.7 for system ERM requirements for structured electronic recordkeeping systems.
- (13) Original source records must be maintained for a sufficient time period after digitizing (scanning) to enable the IRS to validate the electronic versions are accurate reproductions, that the metadata is correct, and the target electronic recordkeeping repository is compliant. This time period may vary based on record type subject to risk assessments, quality validation processes, and system backup processes.
- (14) Original source (e.g., paper) records must not be destroyed until digitization validation is approved and a system backup is completed. DPOs need to discuss with IT the backup frequency and the best time to destroy the records. The project plan and/or SOP must specify the period during which paper documents will be retained based on QC/digitization validation confirmation and back up frequency (e.g., paper documents are destroyed 60 days after scanning since QC of backups are performed monthly). Physical destruction (e.g., shredding) of paper must be done in accordance with IRS requirements.

This includes proper shredding methods for sensitive but unclassified (SBU) data, per IRM 10.5.1.6.10.1, Hardcopy Paper Disposition and Destruction.

- (15) The original source records can only be destroyed after **ALL** the following actions have occurred:
- Original paper or microfilm/microfiche has been appropriately digitized and validated by the BU owner of the record material that the digitized versions are suitable replacements,
 - Confirmation by the BU owner of the record material that the digitized versions have been stored in an authorized repository with appropriate security access controls in place,
 - Confirmation by the BU owner of the record material that a system backup involving the digitized versions has occurred,
 - Confirmation by the BU that the digital record can be accessed, fully utilized and/or amended, when appropriate, by any other system requiring access to the digitized record material, and
 - Cleared for disposal by the BU owner of the record material and all stakeholders requiring access to the record (if any).
- Note:** Once the BUs have completed these actions and provided clearance for disposal, the original source paper can be destroyed.
- (16) Prior to destroying original source records that have been digitized, IRS BUs must ensure the requirements listed in 36 CFR 1236 and the IRS minimum digitization technical, metadata, and QC requirements, are met. The digitized version will serve as the official recordkeeping copy and maintained as required by the RCS or GRS. Paper records converted to an electronic medium and provided clearance for disposal can be destroyed as non-record material using Document 12829, GRS 4.5, item 010, or a current NARA-approved RCS **ONLY** when the following scenarios have been met:
- a. Electronic records and associated metadata have been scheduled with NARA,
 - b. All digitization QC standards have been met and verified,
 - c. Electronic records and associated metadata are stored and managed in an approved electronic recordkeeping system,
 - d. Digitized records have been validated to the standards in 36 CFR 1236,
 - e. Paper records are no longer needed for legal, audit or other business purposes, and
 - f. Electronic records and associated metadata have been appropriately backed up.
- (17) In accordance with 36 CFR 1236.36(a) and 36 CFR 1236.40(g), after verifying the validation of digitized records, federal agencies can destroy the original source records if there are NO pending legal constraints on the agency, such as a **litigation hold**. Recipients of litigation hold notices must:
- a. Thoroughly review the hold notice,
 - b. Respond as directed, including an explanation of the format (paper and/or electronically stored information) of the information, and
 - c. Coordinate with their Records Lead to ensure no applicable records (paper and/or electronically stored information) are destroyed (including source records) until the Office of Chief Counsel advises that the original source records are not needed or provides notification that the hold has been lifted.

- (18) Never destroy official business records with subjects that are under active litigation hold. When in doubt about a hold or legal (rights and interests, appeal rights, benefits, national security, or other similar issues) status of specific source records, please consult with the Office of Chief Counsel, Procedure and Administration, prior to destroying the source records after they have been digitized.
- (19) IRS BUs must consult with their Chief Counsel office on the risks of destroying original source records after they have been digitized. Contact the RIM Program office if there is a question regarding appropriate usage of Document 12829, GRS 4.5, item 010, Digitizing Records. GRS 4.5 cannot be applied to:
 - a. Source records whose digitized versions do not meet NARA's digitization standards,
 - b. Permanent source records in formats not yet covered by NARA's digitization standards,
 - c. Permanent source records dated before January 1, 1950,
 - d. Permanent source records with intrinsic value,
 - e. Final digitized versions of records, and
 - f. Input/source records for non-digitized records.
- (20) IRS BUs must transfer validated digitized records to the designated repository and approved paper disposal actions for the original source records as provided for in approved BU files plans. A file plan is a document providing instructions on how a specific organization unit (such as a program office) will organize and maintain its business information.
- (21) In accordance with IRM 1.15.1.3, Oversight Responsibilities, the RIM Program office may review digitization operations and projects to ensure ongoing compliance with applicable records and information management laws, regulations, and policies. Reviews may consist of onsite inspections of storage facilities, procedural/process assessments, or requests for information, to include production requests of original source material for digitized content.

Note: 36 CFR 1236, Subpart D, Digitizing Temporary Federal Records, provides guidelines for digitizing temporary records. 36 CFR 1236, Subpart E, Digitizing Permanent Federal Records, provides guidelines for digitizing permanent records.

1.15.6.17.1
(02-26-2025)
**Digitizing Temporary
Records**

- (1) In accordance with 36 CFR 1236, Subpart D, Digitizing Temporary Federal Records, the following standards must be met:
 - a. Capture all information contained in the original source records,
 - b. Include all the pages or parts from the original source records,
 - c. Ensure the digitized versions can be used for all the purposes the original source records serve, including the ability to attest to transactions and activities,
 - d. Protect against unauthorized deletions, additions, or alterations to the digitized versions, and
 - e. Ensure the digitized versions can be located, retrieved, accessed, and used for the record's entire retention period.
- (2) In addition to IRM 1.15.6.17, digitization projects and operations owners and managers must ensure the 36 CFR 1236.32, Digitization standards, are met when digitizing official temporary records. New digitization projects also must

digitize (scan) official IRS records to meet the IRS minimum technical, metadata, and QC scanning requirements, as well as IRS BU needs.

Note: The RIM Program office (Records office) grants exceptions as needed, based on suitable justification and a thorough assessment of evident and potential risks. Contact the RIM Program office via **Records Management* to discuss the need for a policy exception.

- (3) Digitized records and their associated metadata must be validated to the standards in 36 CFR 1236.34, Validating documentation, in order to replace the original source records. DPOs must contact **Records Management* to start the validation process. DPOs must complete and submit Form 15408, Digitization Validation Assessment, to **Records Management* when digitized versions will replace the original source records as the “official record” or “recordkeeping copy”. Original source records must be maintained for a sufficient time period after digitizing (scanning) to enable the IRS to validate the electronic versions are accurate reproductions, that the metadata is correct, and the target electronic recordkeeping repository is compliant. Once validation has occurred and the system has been backed up, stakeholders can destroy the original source records. Validation documentation must be maintained for the life of the process, or the life of any records digitized using that process, whichever is longer.
- (4) In most cases, the original source temporary records can be destroyed in accordance with Document 12829, GRS 4.5, item 010, or an appropriate NARA-approved disposition authority, as long as the records are not pending legal action, such as a litigation hold and once the digitized version and associated metadata have been:
 - a. Scheduled with NARA,
 - b. Verified to be an accurate reproduction and suitable quality replacement,
 - c. Designated as the recordkeeping copy,
 - d. Placed in an approved recordkeeping system/repository,
 - e. Appropriately validated,
 - f. Determined by the office/organization that the source records are not needed for other business purposes, and
 - g. Confirmed system backups have occurred.
- (5) Form 11671, Certificate of Records Disposal for Paper or Electronic Records, is not required to destroy the original source records if Form 15408, Digitization Validation Assessment, has been completed and approved. Form 11671 continues to be required for disposal of paper records that have not been digitized.
- (6) The digitized records and their associated metadata must be retained in a NARA-compliant recordkeeping repository for the remaining retention period specified by the applicable NARA-approved RCS (see Document 12990) or GRS (see Document 12829). The records must remain readable, searchable, retrievable, and authentic throughout that period. IRS record owners must designate the digitized version as the **official record** or **recordkeeping copy** on the IRS’s file plan and guidance for staff (e.g., SOPs, IRMs) to distinguish from copies maintained elsewhere.

Note: If you have questions about the appropriate image quality and metadata elements for digitizing temporary records, contact the RIM Program office via

**Records Management.* Additional information can be found in the *Digitizing Temporary Records FAQs* on the RIM KM site.

1.15.6.17.2
(02-26-2025)
Digitizing Permanent Records

- (1) When digitizing permanent records, IRS BUs must contact RIM via **Records Management* prior to the start of the digitization project or operation.
- (2) When digitizing permanent records, IRS BUs must ensure the standards listed in 36 CFR 1236, Subpart E - Digitizing Permanent Federal Records, are met. Subpart E provides the IRS with standards for digitizing permanent paper records and photographic prints (records approved by NARA as having sufficient value to warrant their preservation in the National Archives). This rule also provides the IRS with the guidance necessary to digitize and dispose of source permanent records. Subpart E - Digitizing Permanent Federal Records is outlined in 36 CFR as follows:
 - 1236.40 - Scope of this subpart.
 - 1236.41 - Definitions for this subpart.
 - 1236.42 - Records management requirements.
 - 1236.44 - Documenting digitization projects.
 - 1236.46 - Quality management requirements.
 - 1236.48 - File format requirements.
 - 1236.50 - Requirements for digitizing permanent paper and photographic print records.
 - 1236.52 - Requirements for digitizing permanent mixed-media records.
 - 1236.54 - Metadata requirements.
 - 1236.56 - Validating digitized records and disposition authorities.
- (3) Before starting a digitization project, IRS BUs must establish intellectual control of the records that will be digitized by creating an inventory list as outlined in 36 CFR 1236.42 (a) through (d). The inventory must identify:
 - Whether the records are complete,
 - If there are any gaps in coverage or missing records,
 - The presence of any mixed-media records,
 - The disposition schedule under which the records fall,
 - The date range when the records were created,
 - Any access or use restrictions that apply to the records, and
 - The records' storage location.
- (4) IRS BUs must create digital documentation when digitizing permanent source records. The IRS BU must retain this documentation alongside the digitized records until the digitized records have been transferred to NARA and NARA has notified the IRS that the process is complete. The required documentation will help the IRS populate the TR instrument in NARA's ERA. IRS BUs must follow 36 CFR 1236.44 when documenting digitization projects, including project plans, finding aids, and QC.
- (5) IRS BUs must follow 36 CFR 1236.46 for quality management requirements. This includes meeting the image quality accessioning performance parameters specified in 36 CFR 1236.50 by verifying how well the equipment meets the aim points and tolerances of the parameters. IRS BUs must implement QC inspection and monitoring processes to ensure that images meet the digitization image quality parameters in 36 CFR 1236.50. The IRS BU must also perform QC testing and analysis to identify malfunctioning or improperly configured digitization equipment, improper software application settings, incorrect

metadata capture, or human error, and take corrective actions. The IRS BU must perform QC inspections of the digital records for compliance with the technical parameters and criteria specified in this subpart. The inspection must ensure 100% of the image files:

- Can open and be displayed,
 - Are encoded with a compression type and in a format specified in 36 CFR 1236.48, and
 - Have the resolution, color mode, bit depth, and color profile specified in 36 CFR 1236.50.
- (6) IRS BUs must perform a visual inspection using a statistically valid technique (e.g., a random sample of a minimum of ten digital records or 10% of each batch of digital records, whichever is larger). See 36 CFR 1236.46 for more details.
- (7) IRS BUs must encode, retain, and transfer digitized records in one of the following file formats, either uncompressed or using one of the specified compression codecs in tables 1 and 2 in 36 CFR 1236.48.
- (8) 36 CFR 1236.50 provides the minimum requirements for digitizing permanent paper and photographic print records. IRS BUs must implement appropriate equipment, lighting, special handling, or imaging methods to ensure the capture of all information. The equipment used to digitize federal records must be appropriate for the media type, and capable of achieving documented project objectives without damaging the source records. When digitizing modern textual records, see Table 1 to Paragraph (d) - Requirements for Digitizing Permanent, Modern Textual Paper Records Table and Table 2 to Paragraph (e) - Requirements for Digitizing Permanent, Photographic Print Records and Paper Records That Have Fine Details, listed in 36 CFR 1236.50.
- (9) To ensure that intellectual and physical control of the digital records can be maintained, IRS BUs must follow 36 CFR 1236.54 for metadata requirements. Metadata must be captured in a recordkeeping system, or embedded in each file, or both captured in a recordkeeping system and embedded in each file.
- (10) When validating digitized permanent records, IRS BUs must follow the requirements listed in 36 CFR 1236.56 of these regulations, which also establishes the validation requirements all agencies must fulfill. IRS BUs must not dispose of the original source records until they validate that they have followed the requirements in other sections of the regulation for digitization and QC (among other required assessments during a given digitization project). Once validated, the IRS BU must have an applicable records schedule (e.g., RCS, GRS) that addresses disposing of the original source records after they have been digitized. If the IRS BU validates that its digitization actions meet these new standards, it will be able to use a GRS as authority to dispose of the source records. When IRS BUs follow these standards, they can transfer the digitized records to NARA and destroy the source records. However, destruction is dependent on the IRS having an approved records schedule (e.g., RCS, GRS) to authorize disposition.

Note: Separate staff must conduct the validation, independent from the staff that performed the digitization QC inspections described in 36 CFR 1236.46.

- (11) When IRS BUs work with RIM to transfer permanent records to the National Archives' legal and physical custody, the IRS BU must provide transfer metadata to NARA. The transfer metadata must be entered into the ERA when the TR is created to begin transferring the records. Each transfer of digital records must include the following metadata listed in Table 1 to 36 CFR 1236.58 - Transfer Metadata Table.

This Page Intentionally Left Blank

Exhibit 1.15.6-1 (02-26-2025) Common Questions about Email

When are email messages records?

An email message is a record if:

- It documents the IRS mission or provides evidence of an IRS business transaction, or
- It can be used in other official actions.

Email messages are records unless solely **personal** in content and use, or are non-records. Personal and non-record emails must be maintained separate from official (record) emails.

Note: If the email relates to IRS business or your duties as an IRS employee, it's a record.

Do I have to manage incoming and outgoing email as records?

Yes, you must apply the standard described above to both incoming and outgoing email. The reason is that both the sender and recipient of email messages have the responsibility to document their activities and those of their organizations. Both the sender and the recipient must determine whether a particular email message is a necessary part of that documentation or if it fills in gaps in other records series.

How can email be an official record if it is not signed?

A signature does not make an email a record. Many types of records, such as incoming letters, formal and informal manuals, published reports, photographs, voice recordings, and maps, do not contain signatures, but they can be records.

If an email record is sent to several recipients, which copy is the official record?

It depends. Different copies of the same message may ALL be records. If you take any official action related to a message, and if the message is needed for adequate and complete documentation of the action, the message would be a record in your office, regardless of whether copies are retained elsewhere. If you receive a message for information purposes only and do not take any action related to it, your copy is not a record.

Do these guidelines apply to IRS contractors?

Yes, these guidelines apply to IRS contractors and agents who act on behalf of the IRS, as well as ALL IRS employees. Contract terms must ensure that contractor systems satisfy the legal requirements for creating and maintaining adequate and complete records of IRS transactions when those transactions are carried out by contractors.

Are there special requirements for retaining email messages as records?

The IRS email is managed based on the role of the individual in the organization. However, if the email serves as significant documentation for record sets outside of the email system, such as case files, project files, etc., the email must be associated with the record set outside of the email system and the email in Microsoft Outlook can be deleted.

What if the message does not qualify as a record?

Exhibit 1.15.6-1 (Cont. 1) (02-26-2025)

Common Questions about Email

Delete email that is not a record when no longer needed.

Exhibit 1.15.6-2 (02-26-2025)**Common Questions about Electronic Messaging****What is a record?**

A *record* is anything you create or receive related to your daily work activities.

Are there examples of the types of messages I do not have to save?

Messages that are transitory in nature (or non-record) do not require saving. Examples include:

- “The meeting is about to start. Are you joining?”
- “Do you have time for a quick call before the briefing?”
- “What are you eating for lunch today?”

These routine notifications and reminders are short-term messages with no substantive business information. As such, messages like these do not contain information that needs to be preserved beyond the instant messaging session.

What is instant messaging?

Instant Messaging (“IM” or “IMing”) is the exchange of messages in real-time through a software application. Generally included in the IM software is the ability to easily see whether an individual is available. Instant messaging differs from email because it provides instant feedback.

Can I use instant messaging to send SBU data?

Yes, instant messaging systems are acceptable and convenient methods of automatic encrypted file transmission, but do not supersede policy or work processes for certain programs and offices. To transmit a document from within an IM, click the page-and-paper-clip icon in the upper right corner of your conversation with another user. Follow the instructions to locate the file you wish to transmit. The other party must accept the request for the file to be transferred. Always remember to *Think Data Protection*. Only access or share SBU data or PII with an IRS employee who has a business need for the information. Do not forget that a response to the sending of the instant message could be a federal record and will need to be saved.

What type of messages must NOT be sent using instant messaging?

Employees **should refrain from** using electronic messaging systems to engage in discussions involving policy matters, business decisions, or documentation of other mission-critical functions.

If I use electronic messaging for work, am I creating federal records?

In almost all circumstances, the daily work performed by federal employees (permanent and seasonal) and contractors involves receipt or creation of federal record information.

Is instant messaging the same as text messaging? Am I allowed to use text messaging?

Instant messaging via your laptop is NOT the same as using text messaging on your mobile device or smart-phone. In accordance with IRM 10.8.1.4.1.18.1, Telecommunication Devices, text messaging with government-furnished mobile devices or cellular phones to conduct official business is prohibited, except in emergency situations when other forms of communication are unavailable.

Exhibit 1.15.6-2 (Cont. 1) (02-26-2025)**Common Questions about Electronic Messaging****Is the electronic messaging policy a new requirement?**

No. There has always been a requirement for employees to save and appropriately manage records they create.

May I send an instant message to non-IRS partners/stakeholders or taxpayers?

No. Other than messaging with Department of Treasury officials, IRS's instant messaging application (MS Teams) is an internal application that cannot be used to communicate with others outside of the IRS, including taxpayers.

Who do I contact if I need help saving my instant message or have questions about records management training or other support options?

Please contact **Records Management* if you require training or need assistance with any records-related aspect of using instant messaging.