EFFECTIVE DATE

(03-18-2021)

PURPOSE

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

MATERIAL CHANGES

(1) IRM 1.15.6.1 - Program Scope and Objectives - Expanded the content on managing electronic records in information systems and unstructured data repositories.

(2) IRM 1.15.6.1.1 - Background - Relocated Background content from the Manual Transmittal section to the Background subsection.

(3) IRM 1.15.6.1.2 - Authority - Added content on OMB/NARA M-19-21, Transition to Electronic Records; the Updated Format Guidance for the Transfer of Permanent Electronic Records; the Federal Advisory Committee Act (FACA); and Managing Federal Information as a Strategic Resource.

(4) IRM 1.15.6.1.4 - Definition of Records - Changed the subsection title to correspond with the content.

(5) IRM 1.15.6.1.5 - Acronyms and Terms - Changed the subsection title to correspond with the content. Expanded the list of acronyms and the applicable terms.

(6) IRM 1.15.6.1.6 - Related Resources - Added IRM references for Enterprise Life Cycle (ELC) and IRS Electronic Signature (e-Signature) Program. Also added content on OMB/NARA M-19-21, Transition to Electronic Records.

(7) IRM 1.15.6.2 - Basic Electronic Records Management Definitions - Expanded the list of basic electronic records management definitions.

(8) IRM 1.15.6.4 - Scheduling of Electronic Records - Added new subsection and content communicating that all IRS records, including electronic records, must be scheduled with the National Archives and Records Administration (NARA) before disposition or destruction. Following this newly added IRM subsection, the remaining subsections have been renumbered accordingly.

(9) IRM 1.15.6.5 - Creation, Use, and Maintenance of Structured Electronic Data - Removed content that is no longer applicable (i.e., obsolete Form 12240) and expanded content on the requirements to include records management when acquiring Information Technology Services for creation, use, and maintenance of structured electronic data.

(10) IRM 1.15.6.6 - Creation, Use, and Maintenance of Unstructured Electronic Data - Expanded language on the collaboration needed between the Records and Information Management (RIM) Program office, the Business Units (BUs), and Information Technology (IT) during the creation, use, and maintenance of unstructured electronic data.

(11) IRM 1.15.6.7 - Managing Electronic Mail Records - Relocated content from IRM 1.15.6.7.1.

(12) IRM 1.15.6.7.1 - Email Sent or Received Using Organizational Mailboxes - Changed the subsection title and relocated content from IRM 1.15.6.7.1.1. Added content regarding the owner of the organizational mailbox.

(13) IRM 1.15.6.7.2 - Federal Advisory Committee Act (FACA) Email Records - Added new subsection and content based on Interim Guidance Memorandum PGLD-01-0519-0002, Protecting Federal Advisory Committee Act Records.

(14) IRM 1.15.6.7.3 - Email Sent or Received Using Government-issued Communications Tools - Added some content relocated from the Note portion of IRM 1.15.6.7.5.

(15) IRM 1.15.6.7.4 - Email Created Using Personal or Non-IRS Communications Tools (Bring Your Own Device (BYOD) Program) - Added IRM reference content.

(16) IRM 1.15.6.7.5 - Email Created Using Personal or Non-IRS Communications Tools (not part of the BYOD Program) - Removed and relocated content to IRM 1.15.6.7.3.

(17) IRM 1.15.6.7.7 - Litigation Holds - Added content on the requirement to notify Chief Counsel when under a Litigation Hold and separating from the Service.

(18) IRM 1.15.6.7.8 - System Backups - Changed the subsection title to correspond with the content.

(19) IRM 1.15.6.8 - Judicial Use of Electronic Records - Revised language and expanded content.

(20) IRM 1.15.6.9 - Security of Electronic Records - Updated content on the protection of electronic records restricted from disclosure and the requirement for cloud service offerings to protect federal information.

(21) IRM 1.15.6.10 - Disposition of Electronic Records - Changed the subsection title and expanded the content on the disposition of electronic records.

(22) IRM 1.15.6.11 - Transfer Permanent Records to NARA - Changed the subsection title and updated the content on transferring permanent records to NARA.

(23) IRM 1.15.6.11.1 - Transfer Forms for Permanent Records - Changed the subsection title and updated the information on the forms used to transfer permanent records to NARA using Standard Form (SF) 258, Agreement to Transfer Records to the National Archives of the United States, or through the Electronic Records Archive. Also removed reference to obsolete Form 12240.

(24) IRM 1.15.6.11.2 - Transfer Documentation for Permanent Records - Changed the subsection title and relocated original content to IRM 1.15.6.11.4.2. Included content on providing adequate supporting documentation when transferring permanent records to NARA.

(25) IRM 1.15.6.11.2.1 - Sources of Documentation - Relocated content from IRM 1.15.6.12.1 and expanded the source of documentation that could accompany the transfer of permanent records.

(26) IRM 1.15.6.11.2.2 - Format of Documentation - Relocated content from IRM 1.15.6.12.2 and added content to digitize documentation for electronic records being transferred to NARA.

(27) IRM 1.15.6.11.2.3 - Scope of the Documentation - Relocated content from IRM 1.15.6.12.3 and expanded the content, structure, and context of source documentation. Removed reference to obsolete Form 12240.

(28) IRM 1.15.6.11.3 - Transfer Formats for Permanent Records - Updated the subsection title and the content on the approved formats for transferring permanent records.

(29) IRM 1.15.6.11.4 - Transfer Media for Permanent Records - Added new subsection on the types of media for transferring permanent records.

(30) IRM 1.15.6.11.4.1 - Magnetic Tape - Relocated content from IRM 1.15.6.11.1.

(31) IRM 1.15.6.11.4.2 - Compact Disk, Read Only Memory (CD-ROM) and Digital Video Disk (DVD) - Relocated content from IRM 1.15.6.11.2.

(32) IRM 1.15.6.11.4.3 - File Transfer Protocol (FTP) - Added new subsection on file structures for transferring permanent electronic records to NARA.

(33) IRM 1.15.6.11.4.4 - Electronic Storage Media Maintenance Requirements for Permanent Records - Added new subsection on the environmental conditions for storing permanent and unscheduled records.

(34) IRM 1.15.6.12 - Disposal of Temporary Electronic Records - Added new subsection on disposing of temporary electronic records.

(35) IRM 1.15.6.13 - Use of Social Media - Changed the subsection title and relocated content from IRM 1.15.6.14.

(36) IRM 1.15.6.14 - Use of Collaboration Tools - Changed the subsection title and relocated content from IRM 1.15.6.15.

(37) IRM 1.15.6.14.1 - Use of Agency-approved Electronic Messaging Systems - Relocated content from IRM 1.15.6.15.1.

(38) IRM 1.15.6.14.2 - Preserving Electronic Messages - Relocated content from IRM 1.15.6.15.2.

(39) IRM 1.15.6.15 - Digitization Requirements - Changed the subsection title and added new content on digitization requirements for recordkeeping.

(40) IRM 1.15.6.15.1 - Digitizing Temporary Records - Changed the subsection title and added new content on digitizing temporary records along with the appropriate documentation for recordkeeping.

(41) IRM references, website links, and editorial updates have been made throughout this IRM section.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 1.15.6, dated July 16, 2018. This IRM also incorporates Interim Guidance Memorandum PGLD-01-0519-0002, Protecting Federal Advisory Committee Act Records, dated May 6, 2019.

AUDIENCE

All IRS divisions and functions

Celia Doggette
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
(03-18-2021)
Program Scope and Objectives

(1) **Purpose.** This IRM sets forth policy, assigns responsibilities, and explains requirements for the management of electronic records in accordance with Code of Federal Regulations (CFR) Title 36, chapter XII subchapter B, chapter XII, and United States Code (USC) Title 44, Title 36, chapters 29, 31, 33, and 35.

(2) Managing electronic records in systems and repositories that meet the requirements listed in IRM 1.15.6.1(3), ensures the IRS is compliant with the critical records management policies and regulations as established by the National Archives and Records Administration (NARA) and listed in the CFR. By adhering to these policies, the IRS will also increase business efficiency, and increase the value of information created.

(3) These requirements apply to all IRS electronic information systems and unstructured data repositories. At the IRS, these repositories must:

a. **Store and preserve federal records and associated metadata.** To meet these requirements, repositories must allow users to retrieve and use all records in the repository until the NARA-approved retention period is met.
b. **Manage access and retrieval.** To meet this requirement, 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.** To meet this requirement, PGLD in coordination with repository owners, administrators, and users must: 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.** To meet this requirement, 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.

(4) **Scope.** This IRM section covers the following:

a. Basic requirements for electronic records.
b. Creation, maintenance, retention, and disposition of these records.
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 1.15.6.7, Managing Electronic Mail Records.
e. Recordkeeping requirements when using personal or non-IRS communications tools to conduct IRS business.
f. Basic requirements for digitizing (scanning) temporary records.
g. IRS compliance requirements with NARA records management policies and regulations, improvement in business efficiency and faster responses to litigation and Freedom of Information Act (FOIA) requests.

(5) **Audience.** These procedures apply to ALL IRS employees and contractors.

(6) **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.

1.15.6.1.1
(03-18-2021)
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 information in appropriate recordkeeping systems will ensure that IRS is compliant with all records management policies and regulations as established by the National Archives and Records Administration (NARA). Additionally, management of all agency information (hard copy and electronic) will improve the agency's ability to identify the most current information in a timely manner, increase business efficiency, and provide the correct information for litigation and Freedom of Information (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 its 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 the 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 1.15.6.1.4 for a definition of records, non-records, and personal materials.

(5) The Office of Management and Budget (OMB) and NARA jointly issued OMB/NARA M-19-21, Transition to Electronic Records. This Memo supersedes OMB/NARA M-12-18, Managing Government Records Directive, and provides key targets for Federal agencies to manage both permanent and temporary electronic records, and provides a cutoff date for sending paper records to the Federal Records Centers (FRCs). This IRM provides guidance that will help ensure that IRS records are appropriately managed, retained, and archived, and support the M-19-21 mandates.

(6) RIM will provide assistance and training where necessary on implementing the requirements provided in this IRM.

1.15.6.1.2
(03-18-2021)
Authority

(1) *44 USC Chapters 21, 29, 31, and 33*

(2) 36 CFR Chapter XII Subchapter B, Records Management codes *https://www.govinfo.gov/content/pkg/CFR-2011-title36-vol3/pdf/CFR-2011-title36-vol3-chapXII-subchapB.pdf*

(3) 36 CFR Chapter XII, Subpart B - Part 1222 - Agency Recordkeeping Requirements

(4) 36 CFR Chapter XII, Subpart B - Part 1235 - Transfer of Records to the National Archives of the United States

(5) 36 CFR Chapter XII, Subpart B - Part 1236 - Electronic Records Management

(6) OMB/NARA M-19-21, Transition to Electronic Records *https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf*

(7) *NARA Bulletin 2012-02*, Guidance on Managing Content on Shared Drives

(8) *NARA Bulletin 2013-02*, Guidance on a New Approach to Managing Email Records

(9) *NARA Bulletin 2018-01*, Updating NARA Bulletin 2014-04, Format Guidance for the Transfer of Permanent Electronic Records

(10) *NARA Bulletin 2014-04*, Revised Format Guidance for the Transfer of Permanent Electronic Records

(11) *NARA Bulletin 2014-06*, Guidance on Managing Email

(12) *NARA Bulletin 2015-02*, Guidance on Managing Electronic Messages

(13) *NARA Bulletin 2015-04*, Metadata Guidance for the Transfer of Permanent Electronic Records

(14) 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*

(15) 5 USC Appendix 2 - Federal Advisory Committee Act (FACA), *https://www.govinfo.gov/content/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-app-federalad.pdf*

(16) OMB Circular No. A-130, Managing Federal Information as a Strategic Resource, *https://records-express.blogs.archives.gov/2016/08/02/update-to-omb-circular-a-130/*

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
(03-18-2021)
Definition of Records

(1) 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)

(2) Non-records - work-related documents that do not qualify as records such as duplicate copies, convenience/reference copies, and stocks of publications.

(3) Personal Materials - anything belonging to an individual that is not used to conduct agency business.

1.15.6.1.5
(03-18-2021)
Acronyms and Terms

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

Acronym	Term
BYOD	Bring Your Own Device
CFR	Code of Federal Regulations
ERMT	Enterprise Records Management Taxonomy
FACA	Federal Advisory Committee Act
FOIA	Freedom of Information Act
GRS	General Records Schedules, Document 12829
IM	Instant Message
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
POCs	Points of Contact
PST	Personal Storage Files
RCS	Records Control Schedules, Document 12990
RIM	Records and Information Management
USC	United States Code
FISMA	Federal Information Security Management Act
FEDRAMP	Federal Risk and Authorization Management Program

1.15.6.1.6
(03-18-2021)
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 2.16.1	Enterprise Life Cycle (ELC) Guidance	Standardizes the approach for managing, governing, and supporting projects following the enterprise life cycle throughout the IRS
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	Government Furnished and Personally Owned 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	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): *https://portal.ds.irsnet.gov/sites/vl003/pages/home.aspx?bookshelf=records%20management*
- 44 USC 3301, Definition of a record website: *https://www.archives.gov/about/laws/disposal-of-records.html*
- OMB/NARA M-19-21, Transition to Electronic Records: *https://www.archives.gov/files/records-mgmt/policy/m-19-21-transition-to-federal-records.pdf*
- Document 12829, General Records Schedules
- Document 12990, IRS Records Control Schedules
- *Is It A Record?* flowchart: *https://portal.ds.irsnet.gov/sites/vl003/lists/createandidentifyrecords/landingview.aspx*
- IRS Records and Information Management Program office email at **Records Management* mailbox

1.15.6.2
(03-18-2021)
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. **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.
b. **Capstone** - a roles-based/account-based approach to (electronic) management of email records that allows for the capture of records that should 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).
c. **Collaboration Tools** - used to allow multiple users access to the same document for purposes of sharing information.
d. **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.
e. **Database Management System** - a software system used to access and retrieve data stored in a database.
f. **Data File** - numeric, textual, or graphic information that is organized in a strictly-prescribed form and format.
g. **Digitizing** - the process of converting paper or analog records to electronic records.
h. **Digital Transformation (also known as digitalization)** - the process of converting text, pictures, or sound into a digital form that can be processed by a computer, easily shared, and accessed. It could include comprehensive business process redesign and/or policy updates to reduce and/or eliminate paper.
i. **Disposition** - those actions taken regarding records no longer needed for regular current agency business and documented in Records Control Schedules (RCS).
j. **Disposition Authority** - the legal authorization for the retention and disposal of records.
k. **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.
l. **Electronic Information System** - a system that provides access to computerized federal records and other information.
m. **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.
n. **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.

o. **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).

p. **Electronic Recordkeeping System** - a system whereby records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition.

q. **Electronic Records Storage Media** - material or platform used for the storage of electronic records.

r. **Electronic Transmission Data** - information in email systems regarding the identities of sender and addressee(s), and the date and time messages were sent (sometimes referred to as metadata).

s. **Instant Messaging (IM)** - Instant Messaging (IM) is 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 them to exchange text messages with connected parties in real time. Examples of instant messaging systems include Microsoft Office Skype for Business® and Lync®.

t. **Metadata** - consists of preserved contextual information describing the history, tracking, and/or management of an electronic document.

u. **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.

v. **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.

w. **Social Media** - internet or web-based technologies designed to disseminate information through social interaction. Examples include Facebook, Twitter, Flickr, YouTube, and other such technologies.

x. **Structured Electronic Data** - electronic data that resides in fixed fields within a record or file such as relational databases.

y. **Text Message** - an electronic communication (aka Short Message Service, SMS) sent and received by a mobile phone or other similar device.

z. **Unstructured Data Record Content** - unstructured data that meets the criteria of a federal record as defined in 44 USC 3301.

aa. **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.

ab. **Unstructured Data Repository** - a digital system or directory primarily used to store or collaborate on unstructured data such as SharePoint. Such repositories may or may not be equipped with out-of-the-box records management functionality.

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

(1) The National Archives and Records Administration (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 Code of Federal Regulations (CFR) Part 1236, Electronic Records Management, is available at *https://www.govinfo.gov/content/pkg/CFR-2011-title36-vol3/pdf/CFR-2011-title36-vol3-chapXII-subchapB.pdf*.

1.15.6.4
(03-18-2021)
Scheduling of Electronic Records

(1) A Records Control Schedule (RCS) 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 (44 USC 3303) with NARA. The records must be covered by an agency schedule or a General Records Schedule (GRS). Records Control Schedules are available for each IRS major function and are published in IRS Document 12990. General Records Schedules are used by the IRS and other federal agencies for most administrative records requirements with some minor modification to certain series to comply with various Government Accountability Office (GAO) and Department of the Treasury specific requirements, and the GRS are published in Document 12829. Without an approved schedule, records are not authorized for destruction and must be held until a schedule is approved by the Archivist of the United States.

(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:

a. Scheduling all electronic records, including masterfiles, related documentation and indexes, by submitting a new request for records disposition authority to the RIM Program office, or in some instances, by applying NARA's GRSs. The information in electronic information systems, including those operated for the IRS by a contractor, must be scheduled as soon as possible, but no later than one (1) year after implementation of the system.
b. Transferring permanent electronic records and related documentation and indexes to NARA at the time specified in the Records Control Schedules for permanent records.
c. Providing guidance for the destruction or other disposal of temporary electronic records no longer having sufficient administrative, legal, research or other value warranting their further retention.

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

Note: All RCS dispositions must be reviewed and approved by the IRS Records Officer and NARA prior to implementation and use by the IRS. 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.

1.15.6.5
(03-18-2021)
Creation, Use, and Maintenance of Structured Electronic Data

(1) In accordance with *OMB Circular A-130* and *NARA Universal Electronic Records Management (ERM) requirements*, records management requirements must be incorporated into the design of new electronic systems that produce, use, or store data files. Contact the RIM Program office at **Records Management* for requirements information.

a. Acquisitions of Information and Technology Services must include records management requirements in solicitations. See NARA's basic recommendations for RIM contract language, *https://www.archives.gov/records-mgmt/policy/records-mgmt-language*.
b. IT Investment Design and Management must fully incorporate records management functions, retention and disposition requirements into infor-

mation life cycle 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. The RIM Program office must participate in the Systems Development Lifecycle (SDL) and Capital Planning and Investment Control (CPIC) processes to ensure permanent electronic records are appropriately identified and scheduled.

(2) Legacy/existing systems must be reviewed by the RIM Program office to ensure compliance with NARA electronic recordkeeping requirements.

(3) IT and IRS offices must maintain adequate and up-to-date technical documentation for each electronic system that produces, uses, or stores data files.

(4) Electronic System Shutdown (related to projects that follow the Enterprise Life Cycle (ELC) process). Electronic system owners must follow appropriate shutdown procedures when a system is scheduled for cancellation. Any records that have not yet met their required retention periods must be migrated into an 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:
i. Notify the RIM Program office of changes to system (i.e., name change, or changes in functionality, etc.);
ii. Determine if any changes should be made to the disposition of the new system based on changes in functionality; and
iii. 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:
i. Notify the RIM Program office that this information will no longer be collected; and
ii. Establish a plan to manage any legacy record data that has not yet met its approved disposition.

1.15.6.6
(03-18-2021)
Creation, Use, and Maintenance of Unstructured Electronic Data

(1) **Records and Information Management Program Office Responsibilities.**

a. **Configure Records Management Controls.** RIM Program office is responsible for assisting Business Units with the implementation of appropriate records management controls (see 36 CFR 1236.20(b), Electronic recordkeeping) to ensure that all unstructured data recordkeeping systems are configured appropriately according to the Enterprise Records Management Taxonomy (ERMT) and the Records Control Schedules (RCS). Specifically, this includes:

i. Working with Business Units to prepare, review and approve requirements for any system or repository capable of storing unstructured data.

ii. Overseeing the association of unstructured data record content to an approved records schedule and disposition instruction according to 36 CFR 1236.20(b)(3), Organize records.

iii. Overseeing the preservation of unstructured data record content for as

long as needed to conduct agency business and meet NARA-approved dispositions according 36 CFR 1236.20(b)(6), Preserve records.

iv. Overseeing the deletion of temporary records, and the transfer of permanent, unstructured data record content according to 36 CFR 1236.20(b)(7), Execute disposition.

b. **Create and Manage the Enterprise Records Management Taxonomy (ERMT).** RIM Program office is responsible for developing, maintaining and publishing the ERMT, coordinating with IT to incorporate this tool into unstructured data system or repository design, and educating stakeholders on the ERMT, its effects on the recordkeeping environment, and any subsequent duties required for management. ERMT is a standardized, hierarchical organization schema used to associate electronic records to their respective IRS business function and creator.

c. **Create and Manage Automated Disposition Policies.** RIM Program office is responsible for working with Business Units to ensure the appropriate development, maintenance and publication of automated disposition policies in 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 should be built into unstructured data repositories to the highest extent possible.

(2) **Information Technology Responsibilities.** IT must provide storage locations for unstructured data that meet requirements described under (1a-d) 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 NARA-approved records disposition authorities upon deployment of the system.

(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.). Once all records management functionality is enabled according to IRM 1.15.6.1, these are appropriate platforms to store unstructured electronic records. 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, 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:

i. Ensuring records are covered by NARA-approved dispositions.

ii. Communicating those NARA-approved dispositions to the users of the file share so retention requirements are well understood.

iii. Reviewing annually the file share to take disposition actions required by NARA-approved schedule and document 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 should only be used to store personal material, reference material, 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 (I Drives, MySites, OneDrive, etc.). These storage locations do not currently provide the functionality necessary to electronically manage record information. These individually assigned storage locations should only be used to store working papers or reference material that do not meet the legal definition of a federal record. All federal records must be moved to a compliant Document Management System/Collaboration Environment.

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 may be used to transfer record to an approved recordkeeping system or to back-up material saved to a hard drive.

   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 should include the Business Unit/employee name, the applicable Records Control Schedules 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) may grant 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, Examination of Returns, Workpaper System and Case File Assembly and IRM 4.33.1, Electronic Business, Managing Electronic Records from Taxpayers and Third Parties). Contact the RIM Program office at **Records Management* to discuss the need for a policy exception.

f. 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 office at the **Records Management* mailbox.

1.15.6.7
(03-18-2021)
Managing Electronic Mail Records

(1) **IRS Role-based Approach Explained** - Under the IRS role-based approach, IRS manages email records based on the role of the email account user and/or office rather than on the content of each email record. Email records are captured and managed according to user role using the following retention approach:

Role	Position	Email Records Management
Senior Officials	• Commissioner • Deputy Commissioners • 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	IRS will retain permanent email records according to the approved email records schedule and then accession them into the National Archives of the United States. ***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.
All other IRS employees		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) and maintain according to the Document 12990, IRS Records Control Schedules or Document 12829, General Records Schedules. 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, 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.

1.15.6.7.1
(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 Business Unit correspondence. A shared mailbox has mail 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 should not be used for personal communications (emails strictly personal in nature and not related to agency business), and if they are, must be deleted immediately after close of discussion thread.
d. Capstone officials may 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 overall management of the mailbox. The mailbox owner must establish business use rules and ensure compliance with agency and organizational policy for assigning emails, tasking email responses, and preserving the emails as appropriate.
f. Organizational mailboxes do not have archive mailboxes. An owner may 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 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 tasked for response, and response due date.

d. The employee tasked to respond must ensure his/her 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.

1.15.6.7.2 (03-18-2021) **Federal Advisory Committee Act (FACA) Email Records**

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

a. Email may be used for all informal and formal business communications and collaborations among FAC members, with 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 under *General Records Schedule (GRS) 6.2*, Federal Advisory Committee Records, for Federal Advisory Committee Act (FACA) Records, all IRS FAC members must copy a designated committee organizational mailbox address for all substantive FAC-specific business emails.
b. 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. Excluded from this sub-set of substantive (permanent) committee member communications are 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 should 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 *GRS 6.2*, Federal Advisory Committee Records).
b. The DFO (or other designated committee official) should 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, 29–33*, and regulations issued by the National Archives and Records Administration (NARA). [41 CFR 102-3.175(e) Advisory committee records]

1.15.6.7.3
(03-18-2021)
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 sections.

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, Privacy Policy, for details on emails with personal accounts.

1.15.6.7.4
(03-18-2021)
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 BYOD will be managed in accordance with the account-based email policies set forth in previous sections. Refer to IRM 10.8.26, Government Furnished and Personally Owned Mobile Device Security Policy.

1.15.6.7.5
(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, Information Technology (IT) Security, Policy and Guidance, and IRM 10.5.1, Privacy and Information Protection, 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.

1.15.6.7.6
(11-23-2016)
Encrypted Email

(1) The Records and Information Management (RIM) Program office will provide oversight for the following:

- For email accounts containing permanent email, work with the appropriate Business Unit 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.

1.15.6.7.7
(03-18-2021)
Litigation Holds

(1) For email accounts subject to litigation holds (IRM 25.3.1, Litigation and Judgments, General Guidelines and *IRM 34.7.1*, Pre-Trial Procedures, 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 Service, 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 Information Technology 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.

1.15.6.7.8
(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 agency electronic recordkeeping system.

(2) Backup systems must adhere to prescribed management requirements as defined in Document 12829, General Records Schedules, GRS 3.2 items 040, System backups and tape library records and 050, Backups of master files and databases.

1.15.6.8
(03-18-2021)
Judicial Use of Electronic Records

(1) Electronic records may be used as digital evidence for use in court proceedings, provided the electronic records have established "trustworthiness" as set forth in the Federal Rules of Evidence 803(8). 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 life cycle, the maximum time span that records remain on each storage medium, and the NARA-approved disposition of all records; and
d. Coordinate all of the above with the Office of Chief Counsel, the IRS Records Officer and senior records management staff.

1.15.6.9
(03-18-2021)
Security of Electronic Records

(1) IT and IRS offices with responsibility for electronic records will 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 agency personnel are trained to safeguard sensitive or classified electronic records.
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 Management Act (FISMA), the Computer Security Act, and other statues, 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.

1.15.6.10
(03-18-2021)
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 in office space to conduct current agency 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 agency business, usually by destruction or occasionally by donation.

1.15.6.11
(03-18-2021)
Transfer 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 paragraphs below. If you need additional guidance after confirming your records retention and disposition authority in the IRS Records Control Schedules, consult the IRS RIM Program office or your BU IRC for more detailed instructions and guidance on the transfer of permanent IRS records.

1.15.6.11.1
(03-18-2021)
Transfer Forms for Permanent Records

(1) The form required to transfer permanent records (hard copy and electronic) to NARA is the *Standard Form (SF) 258*, Agreement to Transfer Records to the National Archives of the United States, or a completed Transfer Request (TR) via the Electronic Records Archives (ERA). See IRM Exhibit 1.15.5-1 for a sample SF-258.

(2) Contact your Records Specialist found at *https://portal.ds.irsnet.gov/sites/vl003/lists/recordsspecialists/landingview.aspx* or the RIM Program office for instructions and assistance in completing the form and identification of 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) 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. 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 Business Units must provide the metadata elements as an index in a machine-readable CSV file. IRS must notify NARA if there are additional metadata provided with the transferred permanent records.

1.15.6.11.2 (03-18-2021) **Transfer Documentation for Permanent Records**

(1) Per 36 CFR 1235.48, What documentation must agencies transfer with electronic records, 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. 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 or statistical files and from that for 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.

1.15.6.11.2.1 (03-18-2021) **Sources of Documentation**

(1) Sources of documentation might be 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.

1.15.6.11.2.2 (03-18-2021) **Format of Documentation**

(1) Some of the documentation for electronic records may only exist in paper form and may need to 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.

1.15.6.11.2.3 (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?" and "Why?" and "For What Purpose?"
d. If several data files containing related information are transferred, the documentation should include a description or diagram of how the files relate to each other. At a minimum, the documentation should 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.

1.15.6.11.3
(03-18-2021)
Transfer Formats for Permanent Records

(1) NARA determines which sustainable formats are acceptable for transfer. NARA has identified preferred and acceptable formats for each category in tables found at *https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html*. IRS Business Units 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 should have standard ANSI labels as specified in Federal Information Processing Standard (FIPS) Publication 79 and/or 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 should have the same logical format. Each data element within a record should contain only one data value. A record should 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 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 at *http://www.archives.gov/records-mgmt/policy/transfer-guidance.html*.

1.15.6.11.4 (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 file transfer protocol (FTP).

1.15.6.11.4.1 (03-18-2021) **Magnetic Tape**

(1) IRS offices may transfer electronic records to NARA on magnetic tape using either open-reel magnetic tape or tape cartridges. Open-reel tape should be on $\frac{1}{2}$ inch 9-track tape reels recorded at 1600 or 6250 bytes per inch and blocked no higher than 32,760 bytes per block. Tape cartridges should be 18-track 3480-class cartridges recorded at 37,871 bpi and blocked at no more than 32,760 bytes per block. If DLT tape IV cartridges are used, the data must be blocked at no more than 32,760 bytes per block and 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.

1.15.6.11.4.2 (03-18-2021) **Compact Disk, Read Only Memory (CD-ROM) and Digital Video Disk (DVD)**

(1) CD-ROMs may be used as transfer media for fielded data files or text files if they conform to the International Standards Organization (ISO) 9660 Standard and to the American Code for Information Interchange (ASCII); are not compressed unless NARA has approved the transfer of the compressed form in advance; and are individually addressable. The CD-ROM may contain software files and temporary records, but permanent records must be in files that contain only permanent records.

(2) DVDs may 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.

1.15.6.11.4.3 (03-18-2021) **File Transfer Protocol (FTP)**

(1) IRS may use File Transfer Protocol (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 with a signed Transfer Request (TR) or *SF 258*, Agreement To Transfer Records To The National Archives of the United States, sent to NARA's Electronic Records Division. The RIM Program office will assist with completing all required forms.

(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.

1.15.6.11.4.4
(03-18-2021)
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 should be assessed and tested regularly to check for degradation, and information should be transferred to new storage media before loss of quality or technological obsolescence occurs. If there is evidence of file corruption, data should be migrated to new media.

(2) IRS Business Units must maintain areas with electronic records storage media containing permanent and unscheduled records 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 Business Units should adhere to the media manufacturer's recommendations for specific environmental conditions in which the media should be stored.

(3) IRS Business Units 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 Business Units 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 are ten (10) years old, IRS Business Units 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 may be destroyed with approval from the IRS RIM office. The IRS Business Units 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 should have a physical label; data stored on a server should be indexed). IRS Business Units should 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.

1.15.6.12
(03-18-2021)
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 Business Units may 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 Business Units must destroy the records in accordance with the records schedule.

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

1.15.6.13
(03-18-2021)
Use of Social Media

(1) IRS must manage record material produced or posted using social media such as Facebook, YouTube, 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 Records Control Schedule (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 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*.

1.15.6.14
(03-18-2021)
Use of Collaboration Tools

(1) IRS must ensure the proper management of record material produced using collaboration tools (e.g. wikis, blogs, web portals, etc.). Collaboration may happen in multiple contexts, such as person to person, office to office, agency to agency, or public to agency (i.e., via interactive websites).

(2) The following records management considerations must be addressed with the use of these technologies:

a. Information that meets the statutory definition of a federal record (44 USC 3301) must be captured and managed in accordance with an approved RCS.
b. Records must be captured in an accessible, usable format.
c. If the collaboration is not located on the agency's network, the Business Unit must discuss procedures for the capture of record material with the IRS Records Program office via **Records Management*.

Note: This guidance does not cover voicemail/Viewmail or the exchange and sharing of real time information through Live Meeting, group training sessions or similar functions of a collaboration system. Business Unit creators are responsible for the official maintenance of training/presentation/briefing materials shared (or updated) using Live Meeting or screen shares. The instant messaging software server is not the recordkeeping repository for those documents, and copies maintained by meeting participants would be considered reference material eligible for destruction when no longer needed.

The Business Unit initiating a Live Meeting or share session to conduct business must make a decision as to the most appropriate method for documenting the session, such as an audio recording or written minutes. All official meeting records including the agenda, minutes, handouts, presentation materials, and recordings, should be maintained outside the session by the host Business Unit in association with an approved disposition authority for that office.

1.15.6.14.1
(03-18-2021)
Use of Agency-approved Electronic Messaging Systems

(1) Email should be used for official business. Guidance for the management of email records is found in IRM 1.15.6.7, Managing Electronic Mail Records. See also IRM 10.5.1, Privacy and Information Protection, Privacy Policy, Email.

(2) Electronic messaging systems (for example, Microsoft Office Skype for Business®) **should only** be used for informal business communications and collaborations. Examples of suitable use include, but are not limited to:

a. Real-time, quick communications among employees relating to requests for information/status that require no follow-up actions or business decisions and do not form the basis for action or decision, such as communications to inform an employee that a document is ready for signature, a request to review draft work products (including attachments), or to inquire about an employee's availability for a phone call or meeting.
b. Casual reminders, such as notification about a change to one's schedule, reminder of a deadline, or scheduling of work-related trips and visits.

(3) Employees **should not** use electronic messaging systems to engage in discussions regarding policy matters, business decisions, or documentation of other mission-critical functions. This will result in the creation of a federal record that requires preservation beyond the closeout of the instant messaging session. Examples of unsuitable use include, but are not limited to:

a. Communications documenting IRM reviews and policy approvals, or decisions.
b. Discussions about examinations and/or case processing and resolution.
c. Communications regarding personnel matters and performance (e.g., disciplinary actions, disputes, or grievances).

(4) In accordance with IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, Telecommunication Devices on the use of text messaging with government-furnished mobile devices or cellular phones to conduct official business is prohibited. Text messaging may only be used in emergencies, such as when the IRS network is down and there is an urgent need to communicate or in disaster recovery situations.

(5) Electronic messages 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, Information Technology (IT) Security, Policy and Guidance. 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. Only access or share SBU data or PII with an IRS employee who has a need for it in performing official duties.

(6) The following chart includes some examples of unsuitable use of instant messaging systems:

Unsuitable Use of Instant Messaging			
If message pertains to...	**Such as...**	**Then...**	**Why**
Requests for managerial approvals in connection with examination or case-related decisions, closing actions or requests to assert penalties	I am on a call and I think I can obtain compromise. I just finalized my review of the file and wanted to know if I could ask your approval of a recommended course of action.	Instant Messaging should not be used.	Instant Messaging should not be used for policy determinations, decisions, or documentation of other mission-critical functions. If used in this manner, the message must be preserved in association with related records and in accordance with applicable records schedules.
Personnel or performance matters	I want to know why I did not get an Outstanding on my annual performance appraisal. I would like to request two days off next week.	Instant Messaging should not be used.	Instant Messaging should not be used to document or review personnel or performance matters. If used in this manner, the message must be preserved in association with related records and in accordance with recordkeeping guidance found in Document 12829, General Records Schedules.

1.15.6.14.2
(03-18-2021)
Preserving Electronic Messages

(1) This guidance provides specific instructions for preserving instant messages and text messaging. Recordkeeping responsibilities must also be considered when using other electronic messaging systems that are currently available or made available in future deployments.

(2) Instant Messages:

a. Messages that are records with a short-term business need (transitory) do not need to be preserved. Examples of short-term instant messages include, but are not limited to:

i. Personal observation about work-related topics, but not for the conduct of agency business;
ii. Inquiries about availability; and
iii. Quick communications that require no follow-up actions or business decisions and do not form the basis for action or decision.

Note: It is the employee's obligation to ensure messages that are sent or received and determined to be substantive in nature are appropriately preserved (see 2.b. below and Exhibit 1.15.6-2).

b. In the event an instant message is created and is not transitory (see 2.a. above), it must be saved BEFORE the message is closed out. The employee will have the ability to save (Microsoft Office Skype for Business®) messages to the Conversation History folder in his or her Outlook by pressing Ctrl + S.

Note: This guidance is specific to the preservation of records using the chat function of instant messaging systems. Any attachments will not be automatically saved using Ctrl + S. Recordkeeping attachments must be saved to the appropriate case, policy, project, or other business file. All other copies transmitted for sharing or reference purposes do not need to be saved.

c. Once the message is in the Conversation History folder, follow the guidance below:
i. If messages require association with records in another recordkeeping system (as part of a case, policy, project, or other official business file), employees should use the "File, Save As" function or print to PDF to incorporate the instant message into the recordkeeping system.
ii. If messages warrant retention, but not in conjunction with a case, policy, or project file, employees should leave the message in the Conversation History folder, or use their mouse to click and hold the message, move (drag) to the desired location, then release (drop) the message into their inbox or other email folder. In either instance, the message will take on the retention prescribed under the IRS Email Management Policy found in IRM 1.15.6.7, Managing Electronic Mail Records.

d. Instant messages that are subject to a litigation hold, regardless of whether the messages meet the definition of federal records, MUST be saved prior to closing out of the message to ensure their preservation in the event they need to be produced. Messages must be transferred in one of the acceptable manners described in 2.b. above.

e. Instant messages may also be subject to other holds, such as those in connection with congressional inquiries and FOIA requests. These messages MUST be saved prior to closing the message to ensure their preservation in the event they need to be produced. Messages must be transferred in one of the acceptable manners described in 2.b. above.

The following chart contains instant messaging examples when preservation is not required beyond active messaging session.

Records Management Decisions for Agency-Approved Instant Messaging System			
If message pertains to...	**Such as...**	**Then...**	**Why**
Inquiries about availability	Do you have time for a quick call before the briefing? The meeting is about to start. Are you joining? Looks like we need to get ahead of this issue. Please schedule a staff meeting.	Close out session; do not save.	Work-related, short-term in nature. Message does not contain information that is a record, only routine notifications and/or reminders that an action is requested.
Requests for information/ status	I cannot find my copy of the office SOP (standard operating procedures). Can you send me another copy when you get the chance? I sent you draft IRM updates for your review a week ago. Can you please share the status?	Close out session; do not save.	Work-related, short-term in nature. Requests for information or publication require no policy decision or special compilation. Final IRM approval will be officially recorded on Form 2061, Document Clearance Record.
Routine exchanges of information	Just reminding you that I am scheduled to be on leave tomorrow.	Close out session; do not save.	Information communication, not a record of the approved leave, which is recorded in personnel files.

(3) Text Messages (Mobile Communication Devices)

In accordance with IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, Telecommunication Devices on the use of text messaging with government-furnished mobile devices or cellular phones is prohibited, except in emergency situations. In the event of an emergency, users must document the information communicated as records and transfer to an approved recordkeeping system 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. Copies remaining on devices should be deleted immediately after the record has been incorporated into the approved recordkeeping system. All government-owned information is subject to discovery and FOIA.

Note: Text messaging functionality is not available within the Bring Your Own Device (BYOD) program's Good application enterprise environment.

1.15.6.15
(03-18-2021)
Digitization Requirements

(1) IRS Business Units must contact the RIM Program office via **Records Management* prior to the start of large digitization projects to ensure the resolution, size, color, bit-depth, metadata, and other digital capture qualities and image standards are appropriate for the source records being scanned. This requirement is essential for digitizing permanent records.

(2) Paper records converted to an electronic medium may be destroyed in accordance with GRS 5.2, Intermediary Records, **ONLY** when the following scenarios have been met:

a. All standards in IRM 1.15.6.15.1, Digitizing Temporary Records, have been met and verified;
b. Paper records are no longer needed for legal, audit or other business purposes; and
c. Electronic records are stored and managed in an approved electronic recordkeeping system with a NARA-approved retention period.

1.15.6.15.1
(03-18-2021)
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.

Note: Digitization of temporary records must take into consideration 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). 36 CFR 1236, Subpart D, Digitizing Temporary

Federal Records, provides guidelines for digitizing temporary records. Digitizing permanent records guidance is forthcoming.

(2) Digitized records must be validated in order to replace the original source records.

   a. Offices/Organizations must contact **Records Management* to start the validation process.
   b. Validation documentation must be maintained for the life of the process or the life of any records digitized using that process, whichever is longer.

(3) The original source records can be destroyed in accordance with GRS 5.2, Intermediary Records, as long as the records are not pending legal action, such as litigation hold and once the digitized version has been:

   a. designated as the recordkeeping copy,
   b. placed in approved recordkeeping system/repository,
   c. appropriately validated, and
   d. determined by the office/organization that the source records are not needed for other business purposes.

(4) The digitized recordkeeping copy must be maintained in accordance with approved retention requirements.

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*.

Exhibit 1.15.6-1 (07-16-2018)
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 should be maintained separate from official (record) emails.

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

Yes, you should 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 have to 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 should 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?

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.

What if the message does not qualify as a record?

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

Exhibit 1.15.6-2 (07-16-2018)
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 should not save?

Messages that are not substantive in nature 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?"

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 should NOT be sent using instant messaging?

Employees **should not** use electronic messaging systems to engage in discussions involving policy matters, business decisions, or documentation of other mission-critical functions. This may result in the creation of a federal record that requires preservation beyond the closeout of the instant messaging session.

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.

What is the Conversation History folder and where is it located?

The IRS instant messaging system keeps a record of instant message conversations in the Office Outlook Conversation History folder. The Conversation History folder is located in MS Outlook on the left side beneath the Deleted Items folder (just above the Junk email folder).

If I create or receive a record using instant messaging, how do I save it?

Exhibit 1.15.6-2 (Cont. 1) (07-16-2018)
Common Questions about Electronic Messaging

If you create or receive a record using instant messaging, before exiting your conversation, you should save it by selecting Ctrl + S. The message will be placed in your Conversation History folder, you may move it to other folders within Outlook.

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 smartphone. In accordance with IRM10.8.1, Information Technology (IT) Security, Policy and Guidance, Telecommunication Devices on the use of 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.

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?

No. IRS's instant messaging application is an internal application that cannot be used to communicate with others outside of the Service.

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.