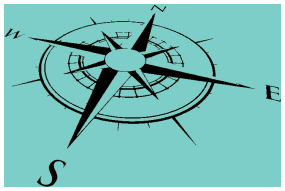
Universal Electronic Records Management (ERM) Requirements

These requirements address born digital electronic records. The requirements are either “program” requirements, relating to the design and implementation of an agency’s ERM policies and procedures, or “system” requirements, providing technical guidance to vendors in creating ERM tools and specifications for agencies to consider when procuring them. Users of this document can filter on "program" or "system" requirements as needed. This could be helpful in finding a list of requirements a system needs to manage electronic records.

The requirements have six sections based on the lifecycle of electronic records management: 1. Capture 2. Maintenance and Use 3. Disposal 4. Transfer 5. Metadata 6. Reporting

Contents



National Archives and Records Administration (NARA)

Stakeholder(s):

NARA Requirements Working Group :
The National Archives and Records Administration's (NARA) Requirements Working Group (RWG) created the Universal Electronic Records Management (ERM) Requirements to: 1. provide standards for agencies and existing Shared Services functional areas to manage their electronic records; 2. help vendors determine capabilities for their ERM tools; 3. help agencies identify the best tools to procure for their needs.

U.S. Federal Executive Branch Agencies

ERM Tool Vendors

Shared Service Providers

Vision

Business needs are met

Mission

To identify requirements for managing electronic records

0. Full Life Cycle

Manage records throughout their full life cycles

0.01. Comprehensiveness

Manage all electronic records

Agencies must manage all electronic records including all recorded information, regardless of form or characteristics, made or received by a Federal agency as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the US Government.

0.02. Access & Permissions

Monitor and review access rights and permission rules for electronic records

Agencies should monitor and review access rights and permission rules for electronic records regularly; these access rights and permission rules should be updated on a regular basis.

0.03. Controls

Monitor and evaluate records controls

Agencies should regularly monitor and evaluate their records controls.

0.04. Responsibility

Retain responsibility for managing electronic records regardless of whether they reside.

Agencies retain responsibility for managing their electronic records, regardless of whether they reside in a public, private, or community cloud; a contracted environment; or under the agency's physical control.

0.05. Use, Alteration, Concealment & Deletion

Prevent unauthorized use, alteration, concealment, or deletion of records

Agencies must have controls to prevent unauthorized use, alteration, concealment, or deletion of records. Examples of controls include audit trails, access lists, monitoring, and agent validation.

0.06. Third-Party Services

Monitor changes to third-party terms of service

Agencies must be responsible for monitoring changes to third-party terms of service that may affect the management of records.

0.07. Agency Business

Provide adequate and proper documentation of agency business

A record must be able to provide adequate and proper documentation of agency business for as long as the information is needed.

1. Capture

Place objects under records management control

The process of placing an object under records management control for disposition and access purposes. Objects are not necessarily moved from the system they reside in when they are captured. Records can be imported from other sources, manually entered into the system, or linked to other systems... A record must be able to provide adequate and proper documentation of agency business for as long as the information is needed.

1.01. Adequacy & Propriety

Provide adequate and proper documentation of agency business

A record must be able to provide adequate and proper documentation of agency business for as long as the information is needed.

1.02. Reliability

Ensure that records provide a full and accurate representation of the transactions or activities

A record is considered reliable if it ensures a full and accurate representation of the transactions or activities.

1.03. Integrity

Ensure records are complete and protected from unauthorized addition, deletion, alteration, use, and concealment

A records is considered to have integrity if it is complete and protected from unauthorized addition, deletion, alteration, use, and concealment.

1.04. Usability

Ensure that records can be located, retrieved, presented, and interpreted

A record is considered usable of it can be located, retrieved, presented, and interpreted.

1.05. Authenticity

Ensure records are what they claim to be

An authentic record is considered authoritative evidence of a transaction or event; records are authentic if they are what they claim to be.

1.06. Agency

Ensure records are created or sent by the agent claiming to have created or sent it

A record must be authentic to be considered authoritative evidence of a transaction or event; records are authentic if they are created or sent by the agent claiming to have created or sent it.

1.07. Events & Actions

Document all events and actions related to records in the system

Once a record has been captured into a records system, all events and actions related to the record by person entities and non-person entities must be documented on an on-going basis.

1.8. Records Schedules

Associate records with records schedules

All records must be associated with the approved records schedules that pertain to each record.

1.9. Social Media Records

Identify and capture social media records

Agencies are responsible for identifying what kind of social media output constitutes a federal record, and capturing those records appropriately.

1.10. Social Media Working Groups

Address the special demands of managing federal records created through social media

Agencies should establish a Social Media Working Group to handle the special demands of managing federal records created through social media.

Stakeholder(s):

Social Media Working Groups

1.11. Social Media Scheduling

Include social media records in records schedules

Agencies must analyze existing records schedules to determine if social media records are covered, and if not, develop an appropriate schedule.

1.12. Electronic Messages

Capture electronic messages within 20 days

Any agency business conducted through electronic messaging accounts are considered Federal records and must be captured within 20 days.

1.13. Searchability

Manage records of current and former employees in a manner that supports searching in response to information requests

Records of current and former employees must be managed in a manner that supports searching in response to information requests, including FOIA and agency business needs.

Stakeholder(s):

Employees **Former Employees**

2. Maintenance & Usage

Manage records through their most active stage

The process of managing records through their most active stage. This includes ensuring records are migrated and transformed as systems change, so the records remain usable. Digital preservation is particularly important for permanent records that will eventually be transferred to NARA... Records of current and former employees must be managed in a manner that supports searching in response to information requests, including FOIA and agency business needs.

2.01. FOIA Queries

Manage records in a manner that allows the searches to be saved for the purposes of supporting sufficiency of search under FOIA

Records should be managed in a manner that allows the searches to be saved for the purposes of supporting sufficiency of search under FOIA.

2.02. Rights & Permissions

Adjust access rights and permission rules for records based upon changes to the legal/regulatory environment, to business activities, or to the structure of the organization

Access rights and permission rules for records should be adjusted to coincide with changes to the legal/ regulatory environment, to business activities, or to the structure of the organization.

2.03. Functions, Activities & Processes

Base access rights and permission rules for records on the function, activity, or business process related to the records

Access rights and permission rules for records should be based on the function, activity, or business process related to the records. This allows for changes to be made to the organization without affecting the access and permission rules.

2.04. Auditing

Document and track actions changing the level of access, altering records, or changing the location of records

Any actions changing the level of access, altering the record, or changing the location of the record must be documented and tracked into an audit log.

2.05. Usability

Ensure that records are usable for as long as needed

Records must be usable for as long as needed to conduct agency business.

2.06. Sustainability

Maintain records over time

Agencies should have a records sustainability plan to maintain records over time.

2.07. Retention

Determine if the retention period for any records is longer than the life of the system where they are currently stored

Ensuring usability of records means determining if the retention period for any records is longer than the life of the system where they are currently stored.

2.08. Formatting & Metadata

Convert records to usable formats and maintain the link between the records and their metadata through the conversion process

Ensuring usability of records includes converting records to usable formats and maintaining the link between the records and their metadata through the conversion process.

2.09. Migration

Migrate records to new systems before retiring existing systems

Ensuring usability of records includes planning for the migration of records to a new system before the current system is retired.

2.10. Off-Line Records

Ensure that migration of records addresses non-active electronic records stored off-line

Ensuring usability of records includes ensuring that migration of records addresses non-active electronic records stored off-line.

2.11. System Upgrades

Maintain the functionality and integrity of the electronic records when carrying out system upgrades of hardware and software

Ensuring usability of records includes carrying out system upgrades of hardware and software while maintaining the functionality and integrity of the electronic records created in them.

2.12. Cloud Migration

Migrate records to other systems or repositories when cloud providers discontinue services

If their cloud provider discontinues services, agencies must continue to meet their records management responsibilities by migrating the records to another system or repository.

2.13. Security & Controls

Ensure that systems receiving migrated records must have appropriate security and records management controls

The system receiving the migrated records must have appropriate security and records management controls in place to manage the records throughout the entire lifecycle, including preventing the unauthorized access or disposal of records.

2.14. Removal

Ensure proper authorization for removal of Federal records from government custody

Agency personnel must have proper authorization before removing Federal records from government custody.

2.15. Copies

Obtain approval from designated officials before removing copies of records or other non-record materials

Agency personnel must obtain approval from a designated official of the agency, such as the Agency Records Officer or General Counsel, before removing extra copies of records or other non-record materials from government custody.

2.16. Unlawful Actions

Advise NARA of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records

Agencies must contact NARA of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the custody of the agency.

2.17. Technology

Review records schedules to determine if changes in technology affects the value of the records

Agencies must continuously review their records schedules to determine if changes to their use of technology affects the value of the records in question.

2.18. Proactive Release

Manage records in a manner to support proactive release under FOIA

Records must be managed in a manner to support export of records to facilitate access processing under the FOIA or for the purposes of proactive release.

2.19. Business Processes

Review records schedules to determine if changes to business processes affects the value of the records

Agencies must continuously review their records schedules to determine if changes to their business processes affects the value of the records in question.

2.20. Workflows

Configure workflows based on an organization's business process rules and transactional data

Agencies should have the ability to configure workflows based on an organization's business process rules and transactional data, without custom programming.

2.21. Full-Text Queries

Support full-text search of a record content

The records system should allow users to perform a full-text search of a record's content.

2.22. Essential Records

Identify and categorize essential records

The records system must allow agencies to identify and categorize any records considered essential.

3. Disposal

Dispose of records scheduled for destruction

The process of disposing of records scheduled for destruction. Records that meet these conditions are destroyed in accordance with their records retention schedule according to 36 CFR 1226.24 and methods such as those outlined in NIST Special Publication 800-88. Electronic records scheduled for destruction must be disposed of in a manner that ensures protection of any sensitive, proprietary, or national security information... Electronic records must be disposed of in a manner that protects any sensitive, proprietary, or national security information. Any recording media previously used for electronic records containing sensitive, proprietary, or national security information must not be reused if the previously recorded information can be compromised in any way by reuse of the media.

3.01. Deletion

Control deletion of records pursuant to existing records schedules

Agencies must control any proposed deletion of records pursuant to existing records schedules.

3.02. Disposition

Ensure that records are covered by a NARA-approved disposition authority

All records must be covered by a NARA-approved disposition authority. This includes using existing records schedules, creating new schedules, or using an applicable GRS.

3.03. Suspension

Immediately suspend the disposition of records when directed

If a suspend-disposition authority or legal hold is issued, the disposition of approved records must cease immediately. The approved records will remain suspended until a revocation order lifts the authority. Once the authority is lifted, the disposition of approved records can continue.

3.04. Orders, Laws & Justifications

Retain records beyond the period outlined in the records schedule pursuant to court orders, executive orders, laws, or business justifications

Agencies 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.

3.05. Destruction

Destroy records in accordance with records schedules

Once the circumstances pertaining to the extended retention of records are no longer applicable, agencies must destroy the records in accordance with the records schedule.

4. Transfer

Transfer records that have been scheduled as permanent

The process of transferring records that have been scheduled as permanent to the National Archives of the United States. This includes records that have been scheduled as permanent, records that are designated as permanent in a GRS; and, when appropriate, records that are accretions to holdings (continuations of series already accessioned.)

4.01. Formats

Transfer electronic records in formats that are independent of specific hardware or software

Agencies must transfer electronic records in a format that is independent of specific hardware or software.

4.02. E-Mail

Ensure identification of the senders and addressees of email messages

Agencies using an email system that identifies users by codes or nicknames, or identifies addressees only by the name of a distribution list, must include information with the transfer-level documentation to ensure identification of the sender and addressee(s).

4.03. Migrations

Retain records and associated metadata until migrations are completed

During records migration, all records and associated metadata in the originating system must be retained until the migration is complete and the destination system has been deemed reliable and secure.

4.04. Permanent Records

Identify and preserve permanent records regardless of format or location

Agencies must be able to identify and preserve permanent records regardless of format or location for transfer to NARA, when appropriate.

4.05. Passwords & Encryption

Disable passwords or other forms of file-level encryption that prevent access to records

Agencies must disable passwords or other forms of file-level encryption that prevent access to records before transferring permanent records to NARA.

4.06. Custody

Retain permanent electronic records until notified that NARA has accepted custody

Agencies 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.

4.07. Permanent Records

Transfer permanent records to NARA in accordance with records retention schedules

Agencies must transfer permanent records to NARA in accordance with their records retention schedules. Generally, permanent records are transferred between 15 and 30 years after their creation or receipt.

4.08. Formats

Transfer permanent records to NARA in accordance with the preferred and acceptable file formats

Agencies must transfer permanent records to NARA in accordance with the preferred and acceptable file formats outlined in the "Transfer Formats" section of the ERM LoB Requirements Collection. The "Transfer Formats" section is current as of 3/21/2017.

TF.01. CAD

Transfer CAD records in the specified formats

Agencies must transfer CAD records to NARA in the following file formats: preferred file formats are (1) X3D, and (2) STEP; acceptable file formats are (1) PDF/E, (2) U3D, and (3) PRC.

TF.02. Digital Audio

Transfer Digital Audio records in the specified formats

Agencies must transfer Digital Audio records to NARA in the following file formats: preferred file formats are (1) BWF, and (2) FLAC; acceptable file formats are (1) AIFF, (2) MP3, and (3) Wave.

TF.03. Digital Audio

Transfer Digital Audio records according to specification

Digital Audio records must be transferred at a minimum of 16 bits per sample, but 24 bits per sample is preferred. Digital Audio records should also be transferred at a sample rate of at least 44.1 KHz, but a sample rate of 96 KHz is preferred.

TF.04. Digital Cinema

Transfer Digital Cinema records in DPX format

Agencies must transfer Digital Cinema records to NARA in the following file formats: preferred file formats are (1) DPX.

TF.05. Digital Video

Transfer Digital Video records in the specified formats

Agencies must transfer Digital Video records to NARA in the following file formats: acceptable file formats are (1) AVI, (2) MOV, (3) WMV, (4) MPEG 4, (5) MPEG2, and (6) MXF.

TF.06. Digital Photographs

Transfer Digital Photograph records in the specified formats

Agencies must transfer Digital Photograph records to NARA in the following file formats: preferred file formats are (1) TIFF; acceptable file formats are (1) JFIF with JPEG compression, (2) DNG, (3) PNG, and (4) JP2.

TF.07. Scanned Text Formats

Transfer Scanned Text records in the specified formats

Agencies must transfer Scanned Text records to NARA in the following file formats: preferred file formats are (1) TIFF, (2) JP2, (3) PNG, and (4) PDF/A; acceptable file formats are (1) JFIF with JPEG compression, (2) GIF, and (3) PDF/A-2.

TF.08. Scanned Text Images

Transfer Scanned Text images according to specification

For Scanned Text records, Bitonal images must be transferred at 300-600 ppi, with 600 ppi preferred; Gray scale must be scanned at 300-400 ppi, with 400 ppi preferred; Color must be scanned at 300-400 ppi, with 400 ppi preferred.

TF.09. Digital Poster Formats

Transfer Digital Poster records in the specified formats

Agencies must transfer Digital Poster records to NARA in the following file formats: preferred file formats are (1) TIFF, (2) JP2, (3) PNG, and (4) PDF/A; acceptable file formats are (1) JFIF with JPEG compression, and (2) GIF.

TF.10. Digital Poster Images

Transfer Digital Poster images according to specification

For Digital Poster records, Bitonal images must be transferred at 300-600 ppi, with 600 ppi preferred; Gray scale must be scanned at 300-400 ppi, with 400 ppi preferred; Color must be scanned at 300-400 ppi, with 400 ppi preferred.

TF.11. Geospatial Files

Transfer Geospatial records in the specified formats

Agencies must transfer Geospatial records to NARA in the following file formats: preferred file formats are (1) Geo TIFF, (2) GML, (3) TIGER, and (4) KML; acceptable file formats are (1) VPF, (2) ESRI ARC/INFO, TerraGo Geospatial PDF, (3) ESRI Shapefile, and (4) SDTS (imminent transfer format).

TF.12. Presentations

Transfer Presentation records in the specified formats

Agencies must transfer Presentation records to NARA in the following file formats: preferred file formats are (1) ODP, and (2) PDF/A-1; acceptable file formats are (1) PPT, (2) PPTX, and (3) PDF/A-2.

TF.13. Textual Data

Transfer Textual Data records in the specified formats

Agencies must transfer Textual Data records to NARA in the following file formats: preferred file formats are (1) ASCII Text, (2) Unicode Text, (3) ODF, (4) PDF/A-1, and (5) PDF/A-2; acceptable file formats are (1) PDF, (2) DOCX, and (3) DOC.

TF.14. Structured Data

Transfer Structured Data records in the specified formats

Agencies must transfer Structured Data records to NARA in the following file formats: preferred file formats are (1) CSV, (2) ODS, (3) ASCII Text, (4) JSON, and (5) XML; acceptable file formats are (1) MS Excel Office Open XML, (2) XLS, and (3) EBCDIC (imminent transfer format).

TF.15. Data Files & Databases

Transfer data files or databases as flat files or rectangular tables

Data files or databases must be transferred as flat files or rectangular tables. All records in a database, or rows in a relational database, must have the same logical format. Each data element within a record must contain only one data value, and each record must not contain nested repeating groups of data items.

TF.16. DTDs, Schemas & Data Dictionaries

Transfer structured data together with any associated files necessary to verify the validity of the data

Structured data must be transferred together with any associated files necessary to verify the validity of the data, such as DTDs, schemas, or data dictionaries.

TF.17. E-Mail

Transfer Email records in the specified formats

Agencies must transfer Email records to NARA in the following file formats: preferred file formats are (1) EML, and (2) MBOX; acceptable file formats are (1) XML, and (2) MSG.

TF.18. E-Mail Aggregations

Transfer aggregations of Email records in the specified formats

Agencies must transfer aggregations of Email records to NARA in the following file formats: preferred file formats are (1) PST, and (2) MBOX.

TF.19. Web Files

Transfer Web records in the specified formats

Agencies must transfer Web records to NARA in the following file formats: acceptable file formats are (1) WARC, and (2) ARC.

TF.20. HTTP

Ensure that Web records are accessible via HTTP

Web records must be accessible via HTTP from a server to a client browser when a URL has been activated.

TF.21. Web Domains

Transfer together Web content records that share a domain name

Web content records that share a domain name including content managed under format agreement and residing on another site must be transferred together.

TF.22. Web Components

Transfer all component parts of web content records in a manner that maintains all of the original links, functionality, and data integrity

All component parts of web content records that have been appraised as permanent including image, audio, video, and all other proprietary formats, must be transferred in a manner that maintains all of the original links, functionality, and data integrity.

TF.23. Dynamic Content

Transfer Web records with dynamic content in an acceptable format or make them accessible as static content

Web records with dynamic content such as calendars or databases must be transferred in an acceptable format, or be made accessible as static content.

TF.24. URLs

Include all internally referenced URLs when transferring Web records

Web records must include all internally referenced URLs when transferred to NARA.

TF.25. Control Information

Maintain all control information from the harvesting protocol for Web records

Web records must maintain all control information from the harvesting protocol.

TF.26. Calendars

Transfer calendar records in iCalendar / iCal (ICS)

Agencies must transfer calendar records to NARA in iCalendar / iCal (ICS).

5. Metadata

Provide appropriate metadata

Metadata are elements of information that answer the questions 'who, what, where, when, and why' regarding electronic records. Metadata elements provide administrative, descriptive, and technical information that describe the structure and content of electronic records. Metadata elements also provide contextual information that explains how electronic records were created, used, managed, and maintained prior to their transfer to NARA, and how they are related to other records. This information enables NARA to appropriately manage, preserve, and provide access to electronic records for as long as they are needed. Examples include identifier, creator, title, creation date, rights, etc... Metadata for a record must consist of information recording (1) the description of the content of the record; (2) the structure of the record (form, format, and relationships between record components); (3) the business context in which the record was created; (4) relationships with other records and metadata; (5) identifiers and other information needed to retrieve the record; (6) the business actions and events involving the record throughout its existence.

5.01. Definition

Define the necessary metadata

Records systems must define metadata to (1) enable the identification and retrieval of records; (2) associate records with changing business rules, policies, and mandates; (3) associate records with agents, and their authorizations and rights with regards to the records; (4) associate records with their business activities; (5) track processes carried out on records.

5.01.1. Identification & Retrieval

Enable the identification and retrieval of records

5.01.2. Rules, Policies & Mandates

Associate records with changing business rules, policies, and mandates

5.01.3. Agents, Authorizations & Rights

Associate records with agents, and their authorizations and rights with regards to the records

5.01.4. Activities

Associate records with their business activities

5.01.5. Processes

Track processes carried out on records

5.02. Categorization

Categorize metadata

Metadata to manage records must be in one of six categories: (1) Identity - information identifying the record; (2) Description - information determining the nature of the record; (3) Use - information facilitating immediate and longer-term record use; (4) Event plan - information used to manage the record, such as disposition information; (5) Event history - information recording past events on the record and its metadata; (6) Relation - information describing the relationship between the record and other records.

5.02.1. Identification

Identify records

5.02.2. Description

Determine the nature of the record

5.02.3. Usage

Facilitate immediate and longer-term record use

5.02.4. Event Plan

Provide information to manage records, such as disposition information

5.02.5. Event History

Record past events on records and their metadata

5.02.6. Relationships

Describe relationships among records

5.03. Retention & Destruction

Protect metadata from unauthorized deletion and destroy it in accordance with records retention schedules

The metadata for a record must be protected from unauthorized deletion, and must be retained or destroyed in accordance with the record's retention schedule.

5.04. Evidence

Fix and keep metadata as transactional evidence

Once the record has been captured, the associated metadata must be fixed and kept as transactional evidence. The metadata includes a unique identifier, author, date of creation, and relationships with other records.

5.05. Migration

Preserve and transfer metadata with migrated records

When migrating records, all metadata must be preserved and accompanied with the transfer.

5.06. Elements

Include the required metadata elements

Permanent records transfers to NARA must include the following metadata elements: File Name, Record ID, Title, Description, Creator, Creation Date, Rights. Metadata elements such as Coverage and Relation must also be provided if they apply to the records being transferred.

5.07. Indexes

Provide metadata as indexes in machine-readable CSV files

When transferring permanent records to NARA, agencies must provide the metadata elements as an index in a machine-readable CSV file. Agencies must notify NARA if there are additional metadata provided with the transferred permanent records.

5.08. Categorization

Assign records to as many categories as appropriate

Records can represent more than one business activity and therefore can be assigned to more than one record category.

6. Reporting

Generate reports demonstrating effective controls and compliance

Generating reports to allow for further analysis and to demonstrate effective controls and compliance. Reports may include search results, records eligible for disposition, audit logs, and other customized or ad hoc reports... Agencies must have the ability to generate reports demonstrating effective controls and compliance.

6.01. Customization

Design and generate customized reports

The records system should provide the ability to design and generate customized reports.

6.02. Printing

Print reports

The records system should provide the ability to print reports that are legible, professional in appearance, and usable for an agency's official business purposes.

6.03. Filtering & Sorting

Filter and sort report data

The records system should provide the ability to filter and sort report data based on the values contained in any field or column.

6.04. Scheduling & Distribution

Schedule delivery of reports for distribution

The records system should provide the ability to schedule the delivery of reports, and to distribute them to a specified list of recipients.

6.05. Ad Hoc Reports

Design and run ad hoc reports

The records system should provide users the ability to design and run ad hoc reports using any information for which they have been granted access.

6.06. Configurations

Save configurations of ad hoc reports for reuse

The records system should provide the ability to save the configurations of ad hoc reports for reuse.

Administrative Information

Start Date: 2020-04-06
End Date:

Publication Date: 2020-04-10
Source: https://www.archives.gov/records-mgmt/policy/universalermrequirements

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: