March 3, 2022
Incorporating Change 2, February 22, 2024

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
                    DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Directive-type Memorandum (DTM) 22-001 – "DoD Standards for Records Management Capabilities in Programs Including Information Technology"

References: DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended
                DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended
                National Archives and Records Administration General Records Schedule, current edition

<u>Purpose</u>. In accordance with the authority in DoD Directive 5144.02, this DTM:

- Establishes policy, assigns responsibilities, and provides procedures:

  o   For DoD-wide mandatory records and information management requirements for the implementation of information technology (IT) systems and services to inform configuration and technical decisions of acquisition and provisioning programs.

  o   To exploit automation for use, maintenance, and disposition to reduce the recordkeeping burden on IT providers, IT customers, and endpoint users.

  o   To facilitate interoperability, automation, and shared expectations of information governance through more consistent, widely supported, and scalable records management (RM) capabilities.

  o   To mitigate risk to DoD records by establishing consistent retention policy to enable compliance, internal controls, and defensible deletion strategy. In the absence of policy, IT system and service providers make technical assumptions that may conflict with policy and lead to interoperability challenges.

- Is effective March 3, 2022; it must be incorporated into DoD Instruction 5015.02. This DTM will expire effective March 3, 2026.

Applicability. This DTM applies to:

- OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively in this DTM as the "DoD Components").

- IT systems and services before:

     o Granting approval to proceed with the acquisition of a new capability after the publication date of this DTM. Legacy IT will be addressed when this issuance is incorporated into DoD Instruction 5015.02.

     o Provisioning an existing capability to a new customer as of this DTM's publication.

Definitions. See Glossary.

Policy. It is DoD policy that:

- IT systems and services will establish a safe harbor period of up to 30 calendar days for recovering data after user deletion. After the safe harbor period, the data will be irrevocably destroyed.

- IT systems and services will support default disposition policies to plan disposal of all data not assigned disposition authorities. Identification of records and assignment of disposition authorities override any default policies. Default disposition policies allow for the disposal of information that has no business or legal value. See Paragraph 1 of the Attachment for descriptions of the default disposition policies.

- RM functionality will be provided by the IT system or service or provided through an interface to another capability. See Paragraph 2 of the Attachment for what comprises RM functionality.

- Records and record control items will be interoperable when shared or transferred to another IT system or service.
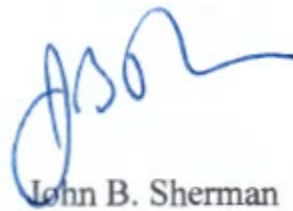
Responsibilities

- <u>DOD CHIEF INFORMATION OFFICER</u>. The DoD Chief Information Officer establishes DoD-wide mandatory records and information management

requirements for the implementation of IT systems and services in accordance with DoD Instruction 5015.02.

- <u>DOD COMPONENT HEADS</u>. The DoD Component heads ensure that DoD standards for RM capabilities are addressed in any applicable IT systems or service.

<u>Summary of Change 2</u>. This change extends the expiration date for the DTM to March 3, 2026.

<u>Releasability</u>. Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

John B. Sherman
DoD Chief Information Officer

Attachment:
As stated

ATTACHMENT

ADDITIONAL DETAILS FOR DOD STANDARDS FOR RM

1. <u>DEFAULT DISPOSITION POLICIES</u>. Default disposition policies for use in DoD IT system and services are listed in Paragraphs 1.a. through 1.d.:

    a. <u>Six-Month Deletion Policy</u>. Data with no business or legal value and low likelihood of contributing to DoD records will be deleted no more than 6 months from the date last modified.

    b. <u>Seven-Year Deletion Policy</u>. Data with no business or legal value but with some likelihood of contributing to DoD records will be deleted no more than 7 years from the date last modified. This likelihood for emerging records is assessed based on the purpose of the IT system or service, the IT component managing that data, and other context for a particular acquisition, development, or provisioning.

    c. <u>Position-Based Retention</u>. IT systems and services will support position-based retention in accordance with National Archives and Records Administration (NARA) General Records Schedule 6.1. This may be extended to other workspaces at the request of the IT customer.

    d. <u>Planning for Default Disposition Policies</u>. At a minimum, before granting authority to proceed or new provisioning, IT providers will provide a cohesive plan for assigning default disposition policies to all data when other disposition authorities are not yet known. This plan will be applied consistently to all data in the IT system or service across the DoD enterprise and included in awareness and training materials. Workspaces, business user case analysis, creating applications, defined content types, and user roles or positions are some target content aspects that may be considered to fully realize capabilities of underlying technology.

2. <u>REQUIRED RM FUNCTIONALITY</u>. RM capability functionality is defined as a set of RM operations given in the table.

    a. Considerations must be taken to ensure that accountable records and information personnel have access and the ability to manage records and information whether by direct access to IT capabilities or through a customer service workflow.

    b. In the case of commercial off-the-shelf product, IT providers and their customers will map these authorized RM-related operations into roles and provide clear documentation and training.

Table. Required Functionality for RM Capability

RM Operation	Considerations for IT Provider	Execution Responsibility
Create, edit, and delete information products.	Applies to non-finalized information products.	End-point user
Find and retrieve information products.	Customer's organizational policies may restrict finding and retrieving permissions based on valid authorization, proper need-to-know, a non-disclosure agreement, or other criteria.	
Manually assign record control items to information products.	• Must be assigned from a defined list. • Assignment overrides any storage location or system-wide defaults.	End-point user where not built into the IT system or service
Finalize records.	When finalized, permission to delete is removed and revisions are versioned.	
Audit information products.	• Actions are logged. • Recommended for customer responsibility.	• Records custodian • Records manager • IT customer technical staff • IT provider technical RM support staff
Change record control item assignment on finalized records.	• Actions are logged. • Recommended for customer responsibility.	
Search and retrieve across all information products, including those in safe harbor.	• Actions are logged. • Recommended for customer responsibility when necessary to support legally authorized search requests.	
Delete non-finalized versions of information products in their custody.	• Actions are logged. • Recommended for customer responsibility.	
Create, find, retrieve, audit, and manage record control items.	Actions are logged.	• Records manager • IT customer technical staff • IT provider technical RM support staff
Make record control items available for assignment.	Actions are logged.	
Execute disposal actions, including coordinating disposition reviews and reporting.	Actions are logged.	
Define, apply, and lift holds.	• Actions are logged. • Applying and lifting holds may be delegated to a records custodian.	
Execute transfer actions for a defined set of information products.	• Actions are logged. • Arrange for transfer of permanent records to NARA.	

Table. Required Functionality for RM Capability, Continued

RM Operation	Considerations for IT Provider	Execution Responsibility
Assign permissions to records storage.	Actions are logged.	• IT customer technical staff • IT provider technical RM support staff
Find, retrieve, and audit user permissions and log files.	Actions are logged.	
Define, manage, and enforce default provisioning templates.	Actions are logged.	
Configure and manage workflows to capture and manage records.	• Actions are logged. • Workflow processes are defined by IT customer functional process owners.	
Configure and manage metadata to support RM.	Actions are logged.	
Configure and manage automation.	Actions are logged.	

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ACRONYM	MEANING
DTM	directive-type memorandum
e-mail	electronic mail
IT	information technology
NARA	National Archives and Records Administration
RM	records management

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
data	Information in a specific representation, usually as a sequence of symbols that have meaning.
disposition authority	An alphanumeric code indicating approval from NARA for records destruction or transfer.
end-point users	Organization staff members or automation that interact directly with IT to perform a business function, including compliance and oversight. End-point users may be restricted to view-only access, but for the purposes of RM, they are assumed to create information products.
IT customer	An organization that pays for an IT system or service, whether internally or externally acquired or shared.
IT provider	An organization supplying systems or services to one or more internal or external customers.
IT service	An IT capability designed to provide awareness of, access to, and delivery of data or information made available for consumption by one or more users. Users can be an individual, organization, or machine.

TERM	DEFINITION
IT system	Complementary networks of hardware and software that people and organizations use to collect, filter, process, create, and distribute data.
NARA General Records Schedule	A schedule issued by the Archivist of the United States to provide disposition authorization for records common to several or all agencies of the Federal Government.
position-based retention	A means of managing and scheduling records and information where final disposition is determined by the role or position of the account user, rather than the value of the content. An example of this approach applied to e-mail is NARA General Records Schedule 6.1.
record control item	A description of a set of records with an associated disposition authority.
records custodian	An organizational staff member who is charged with coordinating hands-on records and information management. They respond to tasking from records managers and component records officers for support in inventory, auditing, disposition reviews, and reporting. If RM is provided as a service, this could be an IT person who executes well-defined and agreed-upon actions on behalf of a service customer.
records manager	An organization staff member who is accountable for executing an organization's records and information program, including coordinating destruction and transfer reviews and retention holds.
safe harbor	A period after destruction of information is requested to allow for lossless recovery of that information.
workspace	A physical or virtual area where work is accomplished. Virtual workspaces include the ability to create, store, share, edit, and destroy digital work products.