

Records Management Policy

Compliance/Organizational Integrity Office – Policy and Records Division

Policy Number: 8236.595
Revised Date: 7/18/2025
Effective Date: 10/14/2025
Issue Date: 9/9/2025

POLICY:

The Department of Human Services (DHS) will make and preserve all records necessary to ensure full and accurate documentation of the official activities of DHS, maintained in a manner that is easily accessible and maintains the protection of information.

AUTHORITY:

[Minnesota Statutes, section 13.03, "Access to Government Data"](#)

[Minnesota Statutes, section 138.17, "Government Records; Administration"](#)

[Minnesota Statutes, section 15.17, "Official Records"](#)

APPLICABILITY:

DHS-wide

Employees may be subject to disciplinary action, up to and including termination, for failure to comply with policies.

PURPOSE:

The purpose of the policy is to establish the responsibilities and processes for managing official records.

DEFINITIONS:

Data categorization: a critical part of data management, which includes identifying and implementing appropriate security controls to support the confidentiality, availability, and integrity of data. The baseline security controls for the protection of the data are grouped as:

Low data is defined by Minnesota Statutes, Chapter 13 as "public" data and is intended to be available to the general public.

Moderate data is defined by Minnesota Statutes, Chapter 13 as "private" or "nonpublic" data and is not intended to be available to the general public. May only be shared with the data subject and those who have a business need to know.

High data is highly sensitive data and/or protected by law or regulation.

Records: government data/information such as cards, correspondence, discs, maps, memoranda microfilms, papers, photographs, recordings, reports, tapes, writings, optical disks, and other data, information, or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received by DHS employees, contractors, or other organizations working with DHS pursuant to state law or in connection with the transaction of public business by an officer or agency. The term “records” excludes data and information that does not become part of an official transaction, library and museum material made or acquired and kept solely for reference or exhibit purposes, extra copies of documents kept only for convenience of reference and stock of publications and processed documents, and bonds, coupons, or other obligations or evidence of indebtedness, the destruction or other disposition of which is governed by other laws. (See Minnesota Statutes, section § 138.17).

Disposition: to complete the lifecycle of a record, usually through destruction or transfer to the Minnesota State Archives.

Convenience copies: copies of correspondence, completed forms, and other records kept solely for the ease of access and reference and must be discarded when they are no longer needed for business use and prior to the disposition timelines of the relevant official record.

Employee: an individual acting as an agent of the Department of Human Services. For the purposes of this policy, employee is read broadly and includes classified employees, unclassified employees, contractors, interns, and volunteers.

Essential information: records or documents, for legal, regulatory, or operational reasons, which if damaged or destroyed would impair the organization’s ability to conduct business and/or require replacement or a need to recreate at considerable expense.

Legal/litigation hold: process by which records that may be relevant to a legal issue are preserved; destruction of records covered by a hold is suspended while the litigation hold is in place.

Official record: government data/information, in any format, made or received pursuant to law or connection with the transaction of public business that represents complete and accurate documentation of the official activities of the agency. The designated official copy of a record that is subject to the records retention schedule.

Record custodian: The individual, position, or business unit responsible for managing a record.

Records Disposition Panel (RDP): a panel consisting of representatives from the State Archives, Offices of Legislative Auditor, and Attorney General’s Office. This group is mandated by Minnesota Statutes, section 183.17 and reviews and approves records retention schedules for Minnesota state agencies and local governments.

Records and information management (RIM) liaison: designated employees from each division/area that liaison between their administrations and the DHS Records Manager, leading RIM efforts in their administrations including developing administration and divisional records retention schedules.

Records retention schedule: An inventory of record types that specifies a time period for the retention and disposition of each type of record.

Unofficial record: copies of official records that are retained elsewhere, convenience copies, informational, or reference copies, records with short-term interest or require no action to be taken and have no documentary or evidential value.

PROCEDURES:

A. Records management

1. All DHS employees:
 - a. must make and preserve all records as evidence of official activities;
 - b. are responsible for collaborating with the record custodians regarding requirements of appropriate retention and storage;
 - c. must communicate the addition or change of official records to the record custodians or RIM liaisons for inclusion on a records inventory and record retention schedule;
 - d. must store official records in the appropriate repository; and
 - e. contact the RIM liaisons for individual administration/division unit guidance.
2. Record custodians:
 - a. are established as the single owner of the record which is documented on the [record retention schedule](#).
 - b. are responsible for collaborating with other agencies, employees, and the DHS Records Manager regarding records management;
 - c. must maintain official records in an arrangement and condition as to make them easily accessible and with the ability to be used in a timely manner;
 - d. must communicate retention requirements to information system designers, managers, or administrators so that systems can be developed to support retention requirements; and
 - e. must protect and preserve records from deterioration, mutilation, loss, or destruction.
3. Supervisors and managers must:
 - a. revise and manage records where a record custodian cannot be identified;
 - b. review and assign management of records to appropriate employees when positions change or when employees leave DHS; and
 - c. consult with the DHS Records Manager or RIM liaison for guidance as needed.
4. RIM liaisons, are responsible for:
 - a. collaborating with employees to increase efficiency by clarifying and recommending cost-effective policies, procedures, tools, and techniques for records and information management;
 - b. reducing redundant systems and information;
 - c. discussing and collaborating between the DHS Records Manager and area employees related to various records management topics, questions, and requirements;

- d. increasing knowledge of employee and county and tribal partners of:
 - 1) how long information needs to be retained;
 - 2) where to find applicable records retention schedules;
 - 3) where to save information; and
 - 4) where to find the information and records they need to do their jobs;
- e. providing county and tribal partners, and employees with current standards and guidance regarding the management of DHS records that are housed elsewhere.

B. Security and access

- 1. Employees must use information appropriately (Refer to [HR/LR Policy 1423, "Appropriate Use of Electronic Communication and Information Technology"](#).)
- 2. Employees must make reasonable efforts to prevent unauthorized access, deterioration, mutilation, loss or destruction of both physical and electronic records.
- 3. Supervisors and managers are responsible for: (Refer to [MNIT standard, "Identity, credential, and access management standard"](#))
 - a. approving requests for information access based on employee's positions;
 - b. reviewing and editing employees' access to systems, storage repositories, and applications based on current positions, transfers, and off-boarding; and
 - c. minimizing record access to the amount needed for employees to complete their responsibilities.
- 4. Record custodians must identify and protect essential information necessary for DHS to continue its key functions and activities in case of an emergency. (Refer to [Business continuity and emergency management](#) webpage.)

C. Record storage and preservation

- 1. Record custodians may designate an electronic version of a record as the official copy.
 - a. Employees must hold records for thirty (30) days after conversion to electronic storage to ensure data integrity.
 - b. Once conversion has been confirmed as accurate, the employee may destroy the paper copies.
- 2. Employees must:
 - a. retain the official record according to the retention schedule;
 - b. store official records in DHS approved storage repositories based on data categorization and statutory classification; and
 - c. store physical records in secure cabinets and in non-public areas pursuant to [Physical and Environmental Security Standards](#), and [Safeguarding Federal Tax Information](#).

3. Off-site storage

- a. RIM liaisons must coordinate with record custodians and assist with paper records that business units no longer need to access frequently.
- b. The off-site storage provider is available to ensure preservation according to approved retention schedules. See [Off-site storage of official agency records](#) for more information;
- c. The DHS Records Manager will coordinate a contract for secure, offsite storage for official records;

4. All employees must:

- a. safeguard records containing sensitive information by storing securely and only granting appropriate access;
- b. limit the amount of sensitive information stored in state email accounts to help ensure any cyberattacks impact as few people as possible;
- c. save documents to a secure location (network drive, SharePoint, FileNet), not the desktop;
- d. encrypt messages containing not-public data to recipients outside of the State of Minnesota Network; ([Refer to “DHS Procedure for Encrypting Emails”.](#))
- e. empty the computer’s recycle bin and email’s sent and deleted items folders on a routine basis; and

D. Retention

1. Employees must:

- a. be familiar with the [DHS General Records Retention Schedule](#) and any applicable business administration/division retention schedules; and
- b. preserve official records according to the retention schedule that applies to them for the full retention instruction period.

2. DHS Records Retention Schedules

- a. The record custodian, DHS Records Manager and RIM liaisons in collaboration must:
 - 1) maintain and review the [General Records Retention Schedule](#) covering official records that are common across multiple business areas;
 - 2) develop or update a [Record Inventory 8236.565b](#) of records the business area stores, creates and receives;
 - 3) update previously existing retention schedules or develop new retention schedules using the information from the Record Inventory 8236.565b and document on the [Minnesota Records Retention Schedule 8236.595a](#);

- a) review the existing retention schedules for accuracy and complete record types/series;
 - b) review and consolidate records on the inventories to combine same retention timeline, same records series and similar items;
 - c) review for inclusion of convenience copies and unofficial records are not required but can be listed on a retention schedule;
 - d) remove or link record types covered by other retention schedules;
 - e) determine retention periods and essential records by:
 - (1) reviewing relevant statute, law, and regulations for retention requirements;
 - (2) reviewing the business unit's mission and activities for the length a record is needed for business purposes;
 - (3) checking the records listed on other DHS retention schedules for consistency of retention timeline; and
 - (4) documenting the retention period that is the longest timeline to store the record.
 - 4) send the completed retention schedule to the business area director for review and approval; and
 - 5) send the completed retention schedule to the DHS Records Manager for review and approval.
- b. The DHS Records Manager must:
- 1) coordinate a review and revision of all records retention schedules at least every 3 years or as soon as practical when new records or retention requirements are identified;
 - 2) contact and submit retention schedules to the Minnesota Historical Society for review and approval by the Records Disposition Panel;
 - 3) act as the liaison between the Records Disposition Panel and the business administration/division employees; and
 - 4) publish approved retention schedules on InfoLink.

E. Litigation Holds and Audits

- 1. The General Counsel's Office will manage litigation holds to preserve records that may be relevant.
- 2. Employees/record custodians notified of any litigation hold must suspend all destruction of the records covered by the litigation hold and maintain the records in their current format. (See the [DHS policy 4000.395, "Litigation Hold Orders"](#).)

3. Employees/record custodians must suspend any record disposition needed to fulfill an active data request or active audit until the audit or active data request is completed.

F. Records disposition

1. Employees in collaboration with record custodians must:

- a. disposition official records that are listed on a retention schedule and have reached the end of the retention timeline;
- b. document the disposition on the [Records Disposition Log 8236.565c](#);
- c. contact a RIM liaison for any official records not listed on a retention schedule;
- d. keep official records not listed on a retention schedule permanently or until a retention schedule has been established; and
- e. destroy courtesy copies and unofficial records when they are no longer needed for business use and prior to the disposition timelines of the relevant official record.

2. Transfer to the Minnesota Historical Society

- a. Employees must not transfer any records to a local historical society, museum, or public library without the specific written permission of the State Archivist from the Minnesota Historical Society.
- b. RIM liaisons or the DHS Records Manager must assist with transferring original official records with archival/historical value to the Minnesota State Archives when their retention schedule states their requirements have been met.
- c. The state archivists will become the owners of the records and are responsible for keeping long-term archival/historical records.
- d. Employees must obtain the state archivists written permission for copies of public records to be made for facility museum display, transferred to a local historical society, museum, public library, or interested individual.

3. Destruction

- a. Employees must properly destroy official DHS records not subject to a litigation hold or audit according to approved records retention schedule(s) instructions, when the records reach the end of their retention period.
- b. Employees must destroy not public information in a way that is unrecoverable.
 - 1) Employees must use appropriate recycle bins and secure bins for shredding of physical records.
 - 2) Employees must delete or erase all content stored on electronic record media (USB drive, tapes, CD's, etc.) before placing in the secured destruction bins located at the loading docks.

G. For quality assurance purposes the DHS Records Manager must:

1. review the records stored offsite yearly for compliance with records retention and storage requirements;
 2. notify business areas with records due for disposition; and
 3. review essential records every three years in conjunction with the retention schedule review.
- H. Training: Employees may complete the Records and Information Management Basic training available on Pathlore.

REVIEW:

Biennial

REFERENCES:

[DHS policy 4000.395, "Litigation Hold Orders" \(PDF\)](#)

[DHS policy 4200.525, "Protecting not public data" \(PDF\)](#)

[DHS policy 8210.140, "Email management" \(PDF\)](#)

[DHS policy 8232.035, "Business continuity management" \(PDF\)](#)

[HR/LR Policy #1423, "Appropriate Use of Electronic Technology" \(PDF\)](#)

[MNIT standard, "Identity, credential, and access management" \(PDF\)](#)

[MNIT standard, "Data Protection Categorization" \(PDF\)](#)

[Business continuity and emergency management \(InfoLink\)](#)

[Information privacy \(InfoLink\)](#)

[Government Records Services | Minnesota Historical Society \(Webpage\)](#)

[Offsite storage for official agency records \(InfoLink\)](#)

[Records and information management \(InfoLink\)](#)

[Records disposal and destruction procedures \(InfoLink\)](#)

[Records management resources and retention schedules \(InfoLink\)](#)

[Records management \(SharePoint\)](#)

[Retention schedule instructions \(SharePoint\)](#)

[Where to store documents by systems \(InfoLink\)](#)

ATTACHMENTS:

[Retention Schedule Template.docx 8236.565a \(Word\)](#)

[Record Inventory Template \(File Plan\).xlsm 8236.565b \(Excel\)](#)

[Records Disposition Log 8236.565c \(SharePoint\)](#)

Records and Information Management Basic (Pathlore)

SUPERSESSION:

DHS policy, “Records Retention and Destruction” effective 7/23/2024 and all policies, memos, or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

Jessica Geil, Chief Compliance Officer
Department of Human Services
Compliance